3/2016

Datenschutz Nachrichten

39. Jahrgang
ISSN 0137-7767
12,00 Euro



Beschäftigtendatenschutz in neuen Gewändern

■ Beschäftigtendatenschutz in neuen Gewändern? ■ EU-US Privacy Shield ■ Das Phänomen Pokémon GO ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



21. und 22. Oktober 2016
Geheimdienste vor Gericht:
Humboldt-Universität und Maxim Gorki Theater Berlin
http://www.ausgeschnueffelt.de

Samstag, 22. Oktober 2016
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 23. Oktober 2016
DVD-Mitgliederversammlung
Bonn.
dvd@datenschutzverein.de

Dienstag, 01. November 2016
Redaktionsschluss DANA 4/2016
Thema: Tracking, Profiling, Werbung, Marketing

Mittwoch, 01. Februar 2017
Redaktionsschluss DANA 1/2017
Thema: Verbraucherschutz

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
39. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Riko Pieper, Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta

Editorial

Gegen Ende des letzten Jahres zeichnete sich bereits ab, dass die DSGVO noch vor Jahresende in ihrer Endversion vorliegen und dann zügig von den verbleibenden Instanzen verabschiedet werden würde. Auch war damals bereits bekannt, dass es zum Arbeitnehmerdatenschutz keine konkreten Regelungen in der DSGVO geben würde, sondern eine von den jeweiligen nationalen Gesetzgebern zu füllende Öffnungs- bzw. Konkretisierungsklausel. Aufgrund der in Deutschland bevorstehenden Bundestagswahl im Herbst 2017 stand somit (rückwärts gerechnet) auch fest, dass die nationalen Anpassungen spätestens gegen Ostern 2017 verabschiedet sein müssen, was wiederum bedeutete, dass sie den entsprechenden Gremien bereits gegen Herbst 2016 vorliegen müssen. Wir gingen somit davon aus, dass die erste Entwurfsversion eines BDSG-Nachfolgegesetzes vor dem Erscheinen des Herbst-Heftes der DANA vorliegen, veröffentlicht und heiß diskutiert werden würde. Somit beschlossen wir, diesem Heft das Schwerpunktthema „Beschäftigtendatenschutz in neuen Gewändern" zu geben.

Es kam jedoch anders: Eine erste Version eines Referentenentwurfs des „Allgemeinen Bundesdatenschutzgesetzes" (ABDSG) ist der DVD tatsächlich kurz vor Redaktionsschluss dieses Heftes in die Hände gefallen und Werner Hülsmann geht darauf in seinem Artikel „Die Europäische Datenschutzgrundverordnung und der Beschäftigtendatenschutz" ein.

Zusammengefasst kann man feststellen, dass das ABDSG bezüglich des Beschäftigtendatenschutzes und der in diesem Zusammenhang auch wichtigen Rolle des Datenschutzbeauftragten folgende Eckpunkte enthält:

- Der § 32 BDSG (Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses) wird in das ABDSG übernommen.
- Der § 3 Abs. 11 (Definition von Beschäftigten) wird in das ABDSG übernommen.
- Die Pflicht zur Bestellung eines DSB ist aus § 4f BDSG sinngemäß übernommen: „…soweit sie in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen"
- Der Kündigungsschutz für DSBs wurde aus § 4f BDSG übernommen.

Über den seit 2009 existierenden § 32 BDSG wurde von Anfang an viel diskutiert – auch in den folgenden Artikeln dieses Heftes. Einerseits sollte der Beschäftigtendatenschutz deutlich umfangreicher geregelt werden als es in diesem einen Paragrafen der Fall ist und andererseits wird von vielen Datenschützern seit Jahren gefordert, den Beschäftigtendatenschutz ganz aus dem BDSG (oder neu ABDSG) zu entfernen und in einem separaten Arbeitnehmerdatenschutzgesetz zu regeln. Dass es wieder einmal nicht (inzwischen seit ca. acht Legislaturperioden) zu dem auch in vielen Wahlkämpfen zugesagten Arbeitnehmerdatenschutzgesetz kommt, ist mehr als ärgerlich. Im aktuellen Koalitionsvertrag war es jedenfalls anders vereinbart und wir haben derzeit eine große Koalition und eine schwache Opposition – noch dazu eine, die sich kaum gegen ein Beschäftigtendatenschutzgesetz sperren würde.

Das Argument, das man aus Regierungskreisen zur Beibehaltung (bzw. Übernahme) des § 32 BDSG derzeit hört ist, dass man die Verabschiedung der DSGVO mindestens zwei Jahre früher erwartet hatte. Dann wäre Zeit gewesen, den Beschäftigtendatenschutz noch in dieser Legislaturperiode grundlegend neu anzupacken. Aber so war dafür halt keine Zeit und das Thema wird (wieder einmal) auf die nächste Legislaturperiode verschoben. Wir werden sehen.

Bezüglich der Kriterien zur Bestellung des DSB und dessen Kündigungsschutz hat die Regierung (jedenfalls bis zum geleakten 1. Referentenentwurf) Wort gehalten. Es wurde immer wieder von deutschen Regierungsvertretern erklärt, dass man an dem in Deutschland erfolgreichen Konzept des DSB und dessen Stellung nichts ändern wollte. Jetzt müssen wir abwarten, ob dies auch so bleibt, bis das Gesetz verabschiedet ist. Viele Datenschutzbeauftragte waren da skeptisch und werden es vermutlich noch ein paar Monate bleiben.

Interessant ist im Zusammenhang mit dem Kündigungsschutz für DSBs, dass die ersten Kommentatoren der DSGVO zu dem Schluss kamen, dass der im BDSG verankerte Kündigungsschutz mit der DSGVO nicht mehr möglich sein wird. Begründet wurde das damit, dass die DSGVO weder einen dem BDSG vergleichbaren Kündigungsschutz vorsieht noch eine Öffnungsklausel dafür. Auch Regierungsvertreter sahen das noch bis vor wenigen Monaten so und stellten die Datenschutzbeauftragten bereits darauf ein, dass sich dieser Punkt wohl nicht aus dem BDSG übernehmen ließe.

Dann fand sich aber doch noch ein Argument, über das sich der Kündigungsschutz trotz der ansonsten vorrangigen DSGVO noch retten ließe: Es wurde argumentiert, dass der Kündigungsschutz für Datenschutzbeauftragte ja gar kein Datenschutzthema wäre, sondern ein Thema des Arbeitsrechts. Darüber sagt die DSGVO jedoch nichts aus, so dass man hierfür auch keine Öffnungsklausel bräuchte[1]. Warten wir ab, ob sich diese Sichtweise aufrechterhalten lässt.

Falls es tatsächlich so bleibt, ist dieser Kündigungsschutz übrigens nicht nur für benannte[2] interne Datenschutzbeauftragte eine gute Nachricht, sondern auch für externe. Für extern benannte Datenschützer gilt ein Kündigungsschutz zwar nicht, denn sie haben ja keinen Arbeitsvertrag. Dafür haben sie aber ein sehr gutes Argument, weshalb sie als Externe unter Vertrag genommen werden sollten. Jedes Ding hat halt seine zwei Seiten.

Für die meisten Autoren dieses Heftes kommt der (bis Redaktionsschluss noch nicht öffentlich verfügbare) Referentenentwurf aber zu spät, so dass der Beschäftigtendatenschutz zunächst ohne Kenntnis der konkreten gesetzlichen Vorgaben aus Deutschland betrachtet werden musste. Hinzu kommt, dass sich vom Referentenentwurf bis zum verabschiedeten Gesetz ja wie schon erwähnt auch noch einiges ändern kann.

Dieses ungeplante Informationsdefizit hatte jedoch den Vorteil, dass die Autoren ganz unvoreingenommen ihre Positionen darstellen konnten, was besonders deutlich in dem Beitrag der Betriebsrätin und Gewerkschafterin (IG Metall) Monika Heim „Persönlichkeitsrechte werden nicht am Werkstor abgegeben!“ zum Ausdruck kommt. Ergänzt wird die Sicht der Arbeitnehmervertretung durch einen Artikel von Lothar Schröder, ver.di- und Aufsichtsratsmitglied (BR) der Telekom, der in seinem Artikel auf „Die Statik des Beschäftigtendatenschutzes“ eingeht.

Auch der Artikel von Karin Schuler und Thilo Weichert über „Vorschläge für ein modernes Beschäftigtendatenschutzrecht“ zählt eine Reihe konkreter Punkte auf, die ein neuer Arbeitnehmerdatenschutz regeln sollte.

Der Artikel der amerikanischen Juristin Jayne Rothman „Transatlantic Compliance: Understanding today’s picture and best practice next steps“ nähert sich dem Beschäftigtendatenschutz über ein anderes aktuelles Thema – dem EU–US Privacy Shield. Ergänzend dazu gibt es auch einen Artikel einer betrieblichen Datenschützerin aus Deutschland, Frau Dr. Kossi, mit dem Titel: „Der Weg zum EU-US Privacy Shield“.

Beide Sichten auf den EU-US Privacy Shield sind aus Unternehmenssicht, zusätzlich stellt Frank Spaeing in seinem Artikel die Position der DVD zum EU-US Privacy Shield dar.

Ein ganz anderes – jedoch genauso aktuelles – Thema, das in diesem Heft mit zwei Beiträgen vertreten ist, betrifft das „Spiel“ Pokémon GO. Im ersten Beitrag stellt Frank Spaeing Pokémon GO in seinen vielfältigen Facetten dar. Im sich anschließenden Artikel mit dem Titel „Die informationelle Selbstenthauptung“ von Roland Appel wird klar, warum das Wort „Spiel“ in diesem Zusammenhang in Anführungszeichen geschrieben werden muss.

Wie immer schließen sich diesen Beiträgen nationale, internationale und technische Datenschutznachrichten an. Danach finden Sie Meldungen zu aktueller Rechtsprechung und abschließend einige Buchbesprechungen.

Eine anregende und informative Lektüre wünschen Ihnen

Riko Pieper und Frank Spaeing

1 Für den Beschäftigtendatenschutz gibt es im Art. 88 DSGVO eine Öffnungsklausel. Die betrifft jedoch die Regelung des Datenschutzes für Beschäftigte und keine arbeitsrechtlichen Aspekte.

2 Die „Bestellung“ nach § 4f BDSG entspricht der „Benennung“ nach Art. 37 DSGVO und heißt somit auch im ABDSG „Benennung“.

Autorinnen und Autoren dieser Ausgabe:

Roland Appel

Jahrgang 1954, lebt und arbeitet als Unternehmensberater und Publizist in Bornheim / Rheinland, www.roaconsult.com und ist Mitherausgeber des „Datenschutz-Führerschein“ www.datenschutz-lernen.de. Von 1990-2000 war er Landtagsabgeordneter und Fraktionsvorsitzender der Grünen in NRW, Roland.Appel@RoaConsult.com

Monika Heim

Betriebsrätin und Sprecherin des EDV-Ausschusses, Mitglied im Ortsvorstand der IG Metall Esslingen, monika.heim@beschds.de

Werner Hülsmann

Vorstandsmitglied in der DVD, Mitglied des Beirats des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., selbständiger Datenschutzberater, externer Datenschutzbeauftragter und Datenschutzsachverständiger, Ismaning und Berlin, huelsmann@datenschutzverein.de

Dr. Victorine Kossi, LL.M.

Referentin Kundendatenschutz DB Mobility Logistics AG, Expertin für internationale Datenschutzfragen und französisches Datenschutzrecht, kossi79@yahoo.de

Neil Watkins

Head of Security and Compliance bei Epiq Systems in Kansas City (Missouri, U.S.). Kontakt über die DVD-Geschäftsstelle

Lothar Schröder

ver.di- und Aufsichtsratsmitglied (BR) der Telekom, lothar.schroeder@verdi.de

Karin Schuler

Informatikerin, freiberufliche Beraterin für Datenschutz, IT-Sicherheit und Mitbestimmung, anerkannte Sachverständige für IT-Produkte, schuler@netzwerk-datenschutzexpertise.de

Frank Spaeing

externer Datenschutzbeauftragter, Vorstandsmitglied in der DVD, spaeing@datenschutzverein.de

Dr. Thilo Weichert

Ehemaliger Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel, Vorstandsmitgied in der DVD, weichert@netzwerk-datenschutzexpertise.de

Werner Hülsmann

Die Europäische Datenschutzgrundverordnung und der Beschäftigtendatenschutz

Beschäftigtendatenschutz in der EU-DSGVO

Die Europäischen Datenschutzgrundverordnung (EU-DSGVO) enthält bedauerlicherweise fast keine direkt wirkenden Regelungen zum Beschäftigtendatenschutz, sondern in erster Linie in Artikel 88 nur eine Konkretisierungsklausel, die es den EU-Mitgliedstaaten ermöglicht durch gesetzgeberische Maßnahme und Kollektivvereinbarungen den Beschäftigtendatenschutz zu regeln und die so Rahmenbedingen vorgibt. Im korrespondieren Erwägungsgrund 155 werden Betriebsvereinbarungen als Beispiel für Kollektivvereinbarungen explizit genannt. Auch in den Begriffsbestimmungen des Artikel 4 EU-DSGVO findet sich keine Definition des Begriffs Beschäftigte, obwohl dieser Begriff in der EU-DSGVO doch mehrmals auftaucht.

„Artikel 88 Datenverarbeitung im Beschäftigungskontext [der EU-DSGVO]

(1) Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

(2) Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

(3) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.“

Auch wenn Absatz 3 Anderes vermuten lässt: Es ist auch nach dem 25. Mai 2018 den Mitgliedstaaten noch möglich, nationale Rechtsvorschriften zum Beschäftigtendatenschutz zu erlassen. Auch diese müssen dann der Kommission unverzüglich mitgeteilt werden.

„Erwägungsgrund 155 [der EU-DSGVO]

Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich ’Betriebsvereinbarungen’) können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.“

Die Beachtung dieses Rahmens sollte dem nationalen Gesetzgeber leicht fallen. Bei der Aushandlung von Kollektivvereinbarungen sieht es dagegen vermutlich etwas schwieriger aus, da bisher bei den datenschutzrechtlichen Bestandteilen von Betriebsvereinbarungen kein vorgegebener konkreter Rahmen zu beachten war. Die Regelungen des BDSG enthalten in diesem Bezug nur abstrakte Formulierungen. Zwar gibt auch das allgemeine Persönlichkeitsrecht der Beschäftigten und das Recht auf informationelle Selbstbestimmung den Rahmen der möglichen Regelungen vor, in der Praxis erfolgte aber auch hier kein direkter Abgleich mit diesen abstrakten Vorgaben.

Planungen der Bundesregierung zur nationalen Gesetzgebung

Die Bundesregierung plant – laut übereinstimmenden Aussagen des BMI und des zuständigen Mitarbeiters der BfDI den § 32 BDSG in die Zeit nach der Ablösung des jetzigen BDSG zu „retten“ und somit zumindest diese minimalistische Regelung zum Beschäftigtendatenschutz weiter gelten zu lassen:

„§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Be-

schäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) (…)

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt."

In dem der Redaktion vorliegenden „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)" mit Stand von Anfang August finden sich diese Passagen im darin als Artikel 1 enthaltenen „Allgemeinen Bundesdatenschutzgesetz – ABDSG" wieder.

Da in der EU-DSGVO gemäß Artikel 4 Absatz 2 nicht mehr zwischen „mit oder ohne Hilfe automatisierter Verfahren" durchgeführter Datenverarbeitung unterschieden wird, wäre der Absatz 2 eigentlich obsolet, findet sich aber im Entwurf wieder.

Die in den § 33 ABDSG-E übernommenen Formulierungen des § 32 BDSG – ergänzt um die Begriffsbestimmung aus § 3 Absatz 11 BDSG – erfüllen zwar die Anforderungen von Artikel 88 EU-DSGVO Absatz 2, nicht aber die Anforderungen an ein Beschäftigtendatenschutzgesetz, das diesen Namen verdienen würde. Es ist zwar besser als nichts, dass die Absätze 1 und 3 des bisherigen § 32 BDSG zum Beschäftigtendatenschutz beibehalten werden, eine wirksame und umfassende Regelung zum Beschäftigtendatenschutz sähe aber anders aus und ist längst überfällig. In den letzten Jahren hat die Bundesregierung die bevorstehende EU-DSGVO und eine eventuell damit einhergehende EU-weite einheitliche Regelungen des Beschäftigtendatenschutzes als Begründung für ihr Nichtstun in Sachen Beschäftigtendatenschutz angegeben. Diese Entschuldigung gilt seit Ende 2015 nicht mehr. Nichtsdestotrotz ist bislang kein Gesetzentwurf zum Beschäftigtendatenschutz seitens der Bundesregierung vorgelegt worden.

Tarif- und Betriebsvereinbarungen zum Beschäftigtendatenschutz

Bereits bisher wurden „Kollektivvereinbarungen", also Tarif- und Betriebsvereinbarungen, die Regelungen zum Umgang mit Beschäftigtendaten enthalten, als „andere Rechtsvorschriften" im Sinne des § 4 Absatz 1 BDSG angesehen. Mit diesen Vereinbarungen konnte und wurde für deren Geltungsbereich der Beschäftigtendatenschutz in den einzelnen Unternehmen oder Unternehmensgruppen geregelt. Durch die Regelung des Artikel 88 Absatz 1 bleibt diese Möglichkeit erhalten. Dabei gibt auch für diese Kollektivvereinbarungen der Absatz 2 des Artikel 88 den Rahmen für derartige Vereinbarungen vor.

Daher sind die in den bereits bestehenden Betriebs- und Tarifvereinbarungen enthaltenen Regelungen dahingehend zu überprüfen, ob sie diesen Anforderungen genügen, damit sie nach dem 25. Mai 2018 Bestand haben. Daher sollte in den Betrieben auf Arbeitgeber- wie auch auf Betriebsratsseite damit begonnen werden, die bestehenden Betriebsvereinbarungen daraufhin zu überprüfen, ob sie den Anforderungen aus Artikel 88 Absatz 2 EU-DSGVO genügen. Betriebsvereinbarungen, deren datenschutzrelevante Bestandteile diesen Anforderungen nicht genügen, sollten rechtzeitig angepasst werden.

Die datenschutzrelevanten Bestandteile der Betriebsvereinbarungen müssen angemessene und besondere Maßnahmen zur Wahrung

- der menschlichen Würde,
- der berechtigten Interessen und
- der Grundrechte der betroffenen Person,

enthalten und dabei insbesondere

- die Transparenz der Verarbeitung,
- die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und
- die Überwachungssysteme am Arbeitsplatz

im Blick haben.

Einzelne verstreute Regelungen zum Umgang mit Beschäftigtendaten in der EU-DSGVO

Übermittlung von Beschäftigtendaten innerhalb von Unternehmensgruppen.

Im Erwägungsgrund 48 wird die Übermittlung von Beschäftigtendaten „innerhalb der Unternehmensgruppe für interne Verwaltungszwecke" ausdrücklich als mögliches berechtigtes Interesse aufgeführt, so dass eine solche Übermittlung gemäß Artikel 6 Absatz 1 Buchstabe f EU-DSGVO zulässig ist, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen".

„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt." (Erwägungsgrund 48 der EU-DSGVO)

In der Praxis wurde und wird in Unternehmen, bei denen kein Betriebsrat existiert und somit auch keine Betriebsvereinbarung vereinbart werden kann, die als „andere Rechtsvorschrift" gelten würde, bislang auch schon die Interessenabwägung gemäß § 28 Absatz 1 Satz 1 Ziffer 2 BDSG als Rechtfertigungsgrundlage für konzerninterne Datenübermittlungen von Beschäftigtendaten für unterschiedliche Verwaltungszwecke herangezogen. Abgesehen davon, dass die Übermittlung von

Beschäftigtendaten zu internen Verwaltungszwecken innerhalb einer Unternehmensgruppen in diesem Erwägungsgrund ausdrücklich als mögliches berechtigtes Interesse angegeben ist, ändert sich vermutlich nichts in der praktischen Umsetzung.

Beurteilung der Arbeitsfähigkeit des Beschäftigten

In Artikel 9 Absatz 2 Buchstabe h EU-DSGVO wird die Verarbeitung von besonderen Datenarten, zu denen u.a. die Gesundheitsdaten gehören, zu Zwecken „der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten" ausdrücklich erlaubt. Die Daten dürfen dabei nur von Personen verarbeitet werden, die einem Berufsgeheimnis (wie z.B. der ärztlichen Schweigepflicht) oder Geheimhaltungspflichten unterliegen, die sich aus EU- oder nationaler Gesetzgebung sowie berufsständischer Verpflichtungen ergeben können. Diese Einschränkung entspricht der Regelung aus § 28 Absatz 7 BDSG. Im BDSG ist allerdings eine Verwendung von Gesundheitsdaten zu Zwecken der Arbeitsmedizin und zur Beurteilung der Arbeitsfähigkeit nicht ausdrücklich genannt. Zumindest die Nutzung von Gesundheitsdaten für die Arbeitsunfähigkeitsbescheinigung ist bereichsspezifisch im § 5 des Gesetzes über die Zahlung des Arbeitsentgelts an Feiertagen und im Krankheitsfall (Entgeltfortzahlungsgesetz)[1] geregelt. Die Arbeitsmedizin ist ebenfalls bereichsspezifisch im Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (Arbeitssicherheitsgesetz, ASIG[2]) geregelt. Von daher ist zu erwarten, dass es in der Praxis keine wesentlichen Änderungen geben wird.

Fazit

Nach wie vor ist der nationale Gesetzgeber gefordert umfassende gesetzliche Regelungen zum Beschäftigtendatenschutz zu erlassen. Er kann sich nun nicht mehr auf anstehende EU-Regelungen berufen. Arbeitgeber sowie Betriebs- und Personalräte sind gefordert die bestehenden Betriebs- und Dienstvereinbarungen – insbesondere deren datenschutzrelevante Inhalte – auf ihren Bestand nach dem 25. Mai 2018 zu überprüfen und gegebenenfalls anzupassen.

1 https://www.gesetze-im-internet.de/entgfg/__5.html

2 https://www.gesetze-im-internet.de/asig/index.html

Karin Schuler, Thilo Weichert

Vorschläge für ein modernes Beschäftigtendatenschutzrecht

Mit Art. 88 der Europäischen **Datenschutz-Grundverordnung** (DSGVO) hat der europäische Gesetzgeber festgelegt, dass die Mitgliedstaaten der Europäischen Union (EU) durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifische Datenschutzvorschriften im Beschäftigtenkontext regeln können. Damit stellt sich für den deutschen Gesetzgeber verschärft die Herausforderung, endlich ein nationales umfassendes Beschäftigtendatenschutzrecht zu schaffen. Entsprechende Versuche waren seit mehr als drei Jahrzehnten immer wieder gescheitert. Auch der Entwurf eines Allgemeinen Bundesdatenschutzgesetzes (ABDSG), welches das bisherige Bundesdatenschutzgesetz (BDSG) als Umsetzungsgesetz der DSGVO ablösen soll, sieht nur eine inhaltliche Übernahme des bisherigen § 32 BDSG in einem § 33 ABDSG vor. Nunmehr stellt sich die Aufgabe, die allgemeinen Prinzipien der DSGVO in Bezug auf die Verarbeitung von Beschäftigtendaten zu spezifizieren. Im Folgenden werden die hierbei relevanten Regelungsthemen sowie die dabei zu verfolgenden Erwägungen und Inhalte dargestellt.

1 Regelungsort

Als **Standort** für ein nationales Beschäftigtendatenschutzrecht wurde von der Bundesregierung bisher das BDSG gewählt. Dies basierte auf der Überlegung, dass eine Konkretisierung der allgemeinen BDSG-Regeln für das Arbeitsverhältnis erfolgt. Diese Annahme ist unzutreffend. Wir haben es hier mit einer Schnittstelle zu tun, die in gleichem Maße Datenschutzrecht und Arbeitsrecht ist. Die dort jeweils bestehenden allgemeinen Regelungen müssen beide vollständig anwendbar bleiben. Das BDSG wäre zudem mit einem eigenen Kapitel, so wie es der Regierungsentwurf 2010 mit den §§ 32 bis 32l vorsah, überfrachtet worden, was nicht zu einer erhöhten Klarheit beigetragen hätte. Um den konkretisierenden Charakter sowohl in Bezug auf das allgemeine Datenschutzrecht als auch auf das Arbeitsrecht herauszustreichen, empfiehlt sich der Erlass eines eigenständigen Beschäftigtendatenschutzgesetzes. Eine Regelung des Beschäftigtendatenschutzes in einem das BDSG ablösenden ABDSG, das ab 2018 in Kraft treten sollte, verbietet sich ebenso, weil ein solches Ausführungsgesetz vorrangig eine generell Ergänzungsfunktion zur DSGVO haben wird. Gemäß den Vorgaben des Art. 88 DSGVO zum Beschäftigtendatenschutz ist eine sehr weitgehende Regelung nötig, bei der nur in bestimmten prozessualen Fragen auf die allgemeinen Regelungen der DSGVO wie einem

noch zu erlassenden nationalen Ausführungsgesetz (künftig also das ABDSG) zurückgegriffen werden kann und muss.

Soweit dies möglich und sinnvoll ist, sollten in diesem Gesetz zu konkreten **Fragestellungen, Anwendungen und Zwecken** gegenüber dem allgemeinen Datenschutzrecht (bisher BDSG, DS-GVO) spezielle Festlegungen vorgenommen werden. Dabei sind sämtliche Regelungsansätze aus den Vorschlägen in der 17. Legislaturperiode des deutschen Bundestags auf den Prüfstand zu stellen, die z. B. zu folgenden Aspekten Aussagen enthalten: Bewerbung, Einstellung, Gesundheitsuntersuchung, Gefahrenabwehr, Strafverfolgung, Videoüberwachung, Ortung/Tracking, Biometrieverfahren, Nutzung von Telekommunikations- und Telemediendiensten (auch soziale Netzwerke) für dienstliche und für private Zwecke, Heimarbeit, Konzerndatenverarbeitung. Auf spezifische Regelungen, die keine sinnvollen und wirksamen Konkretisierungen allgemeiner Vorschriften vornehmen, ist konsequent zu verzichten.

Die gegenüber dem nationalen Gesetz oder der DSGVO zu konkretisierenden Regelungsgegenstände können alles im Beschäftigtendatenschutzrecht erfassen: das materielle Recht ebenso wie die Verpflichtung zu prozeduralen oder technisch-organisatorischen Vorkehrungen. Es sollte darauf geachtet werden, dass diese Regelungen so konkret wie möglich und so offen wie nötig sind. Ziel sollte eine größtmögliche Rechtssicherheit sein, ohne zugleich die sinnvollen Entwicklungsmöglichkeiten der Informations- und Kommunikationstechnik (IKT) zu beschneiden.

2 Kollektivrechte

Neu eingeführt werden sollte die Konkretisierung gesetzlicher Regelungen **auf überbetrieblicher Ebene**. Die hierbei zu treffenden Kollektivvereinbarungen können durch den deutschen Gesetzgeber nur für die Arbeitsverhältnisse in Deutschland vorgesehen werden. Im Interesse möglichst weitgehender europäischer Einheitlichkeit sollte zumindest mittelfristig auch auf europäischer Ebene ein solcher Regelungsansatz verfolgt werden. Gegenstand solcher Vereinbarungen sollte alles sein, was zu einer beschäftigungsspezifischen Präzisierung der allgemeinen gesetzlichen Regelungen führt. So kann es naheliegend sein, branchenspezifische Konkretisierungen vorzunehmen. Denkbar sind aber auch branchenübergreifende Regelungen zu bestimmten Fragestellungen, wie etwa zum Einsatz von Videotechnik oder zur digitalen Zeiterfassung.

Regulatorische Vorbilder für die überbetrieblichen Kollektivvereinbarungen können neben den Regelungen des BetrVG der § 38a BDSG und der Art. 40 DSGVO sein, welche die Anerkennung von **Verhaltensregeln** durch eine Aufsichtsbehörde vorsehen. Anstelle von Verbänden verarbeitender Stellen sollten die Kollektivvereinbarungen in paritätisch von Arbeitgebern und Arbeitnehmern besetzten Gremien erarbeitet werden, die neu zu schaffen wären. Auf der Beschäftigtenseite kommt dabei den Gewerkschaften eine wichtige Funktion zu.

Druckmittel zur Veranlassung von Verhandlungen und Vereinbarungen können gesetzlich geregelte, aufschiebende Vetos sein. Geregelt werden kann auch, dass anlässlich eines konkreten Konfliktes die Pflicht auferlegt wird, eine externe, zu veröffentlichende Expertise einzuholen. Möglich ist die Regelung der Pflicht, eine Aufsichtsbehörde oder einen sonstigen unabhängigen Moderator mit besonderer fachlicher Qualifikation als Schlichter hinzuziehen. Vorbildfunktion könnte das Modell der Einigungsstelle gemäß § 76 BetrVG haben. Initiator für das Verhandeln von Vereinbarungen könnte der unten erwähnte Datenschutzbeirat sein (s. u. 4). Indirekt als Auslöser für Verhandlungen und Vereinbarungen können Medienberichte und Gerichtsurteile wirken.

Parallel dazu sollte die Regelung zur **Mitbestimmung auf betrieblicher Ebene** präzisiert werden. Derzeit sieht z. B. § 87 Abs. 1 Nr. 6 BetrVG bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen," eine Mitbestimmungspflicht nicht nur bei einer gezielten Arbeitnehmerüberwachung vor, sondern auch, wenn eine technische Einrichtung Verhaltens- und Leistungskontrollen ermöglicht. Weitere Mitbestimmungstatbestände mit Bezug zur IKT finden sich in § 87 Abs. 1 Nr. 7 (Gesundheitsschutz) und § 94 BetrVG (Personalfragebögen).

Soweit auf nationaler oder europäischer Ebene eine datenschutzrechtliche **Zertifizierung** von IKT-Produkten und -Verfahren vorgesehen ist, so die Artt. 42, 43 DSGVO, sollte ihre Aufnahme in Kollektivvereinbarungen gefördert werden, verbunden mit einer Privilegierung von zertifizierten Produkten im Rahmen der Einigungsverfahren auf überbetrieblicher wie auf Betriebsebene (vgl. jetzt schon § 9a BDSG).

Einer Schnittstellenregelung bedarf es auch in Bezug auf die **branchenspezifischen Verhaltensregeln**, die durch die Datenschutzaufsicht genehmigt werden können (§ 38a BDSG, Art. 27 EG-DSRl, Artt. 40, 41 DSGVO). Diese kann z. B. darin bestehen, dass die Arbeitnehmerseite in den Genehmigungsprozess der Verhaltensregeln einbezogen wird.

Unabhängig von den oben genannten Klagemöglichkeiten im Rahmen überbetrieblicher und betrieblicher Konflikte sollte auf betrieblicher Ebene für die Beschäftigtenvertretung ein arbeitsrechtliches **Klagerecht gegen die Einführung datenschutzrechtlich unzulässiger IKT-Verfahren** vorgesehen werden. Dies wäre eine sinnvolle normen- und verfahrenskontrollierende Ergänzung zu Art. 80 DSGVO, der u. a. vorsieht, dass in individualrechtlichen Datenschutzkonflikten Betriebsräte oder Gewerkschaften in Vertretung der Betroffenen datenschutzrechtliche Gerichtsverfahren durchführen können. Offen ist, ob es zusätzlich zu der gerichtlichen Entscheidung über Streitigkeiten im Rahmen von überbetrieblichen Vereinbarungen für Gewerkschaften einer Art Verbandsklagerecht bedarf. Mit einem solchen Klagerecht könnte auf Seiten der Arbeitgeber die Bereitschaft gesteigert werden, den Abschluss von Vereinbarungen zu suchen.

Die Regelung des § 8 Abs. 3 BetrVG, wonach der Betriebsrat „bei der Durchführung seiner Aufgaben nach näherer Vereinbarung mit dem Arbeitgeber **Sachverständige** hinzuziehen (kann), soweit dies zur ordnungsgemäßen Erfüllung seiner Aufgaben erforderlich ist", sollte im Hinblick auf die datenschutztechnische und -rechtliche Bewertung präzisiert werden.

Die Rolle der **Datenschutzaufsichtsbehörden** (§ 38 BDSG, Artt. 51 ff. DSGVO) sollte bereichsspezifischer ausgestaltet werden. Es ist vorstellbar, dass diesen als neutralen Stellen eine Mediatorenfunktion zwischen Arbeitgebern und Arbeitnehmern zugewiesen wird. Das bestehende Recht des Betriebsrats, die Aufsichtsbehörde einzuschalten, ohne sich Illoyalität vorwerfen lassen zu müssen, sollte explizit normiert werden. Die Aufsichtsbehörden benötigen für derartige Fragen das Personal und die sonstigen Ressourcen, um innerhalb kürzester Zeit sprech- und antwortfähig sein.

Hinsichtlich der Bestellung und Abberufung von **betrieblichen Datenschutzbeauftragten** (vgl. Artt. 37 ff. DSGVO) sollte der Beschäftigtenvertretung ein Mitbestimmungsrecht eingeräumt werden.

3 Gebote und Verbote

Materiell-rechtlich sollte sich das Beschäftigtendatenschutzrecht auf Aspekte beschränken, in denen ein wesentlicher zusätzlicher Regelungsgehalt zu den allgemeinen Vorschriften erforderlich und möglich ist. Dies gilt u. a. für folgende Themen:

- zusätzliche Freiwilligkeitsanforderungen bei Einwilligungen,
- Benennung der Fälle, in denen eine Einwilligung als Rechtsgrundlage für die Datenerhebung, -verarbeitung und -nutzung ausgeschlossen wird,
- Ausnahmeregelung von einer grundsätzlichen Verpflichtung zur Trennung zwischen privater und dienstlicher Datenverarbeitung,
- die Regelung der privaten Nutzung von dienstlichen Telekommunikationseinrichtungen,
- Nutzungsverbote von Kundendaten von Mitarbeitenden für Personalzwecke,
- Verbot von Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten durch den Arbeitgeber, die aus betriebsärztlichen Untersuchungen stammen.

Hinsichtlich der Abklärung von **Verstößen gegen arbeitsrechtliche Pflichten** sollte ein gestuftes Verfahren vorgesehen werden, bei dem bei Fehlen eines individuellen Verdachtes zur Verdachtskonkretisierung zunächst mit Pseudonymen und Gruppenaggregaten gearbeitet werden muss.

Erwogen werden sollte, inwieweit eine Regelung zur **Benutzung von Beschäftigten-Pseudonymen** in der Außenkommunikation von Beschäftigten möglich und sinnvoll ist.

Zum Recht über die **Personalakte** sollte klargestellt werden, welchen Inhalt eine Personalakte haben darf, welche Aufbewahrungsfristen gelten, wer Zugriff darauf hat, unter welchen Voraussetzungen Aktenbestandteile (über wahre, nachteilige Umstände) zu löschen sind, und welche Anforderungen an die digitale Aktenführung zu stellen sind.

Zum **Whistleblowing** bedarf es nach dem Urteil des Europäischen Gerichtshofes für Menschenrechte vom 21.07.2011 einer spezifischen Regelung. Dabei kann auf eine Vielzahl von schon vorhandenen Vorschlägen zurückgegriffen werden.

Aus Sicht der Arbeitnehmer kann eine Regelung, welche im Beschäftigtenbereich eine **Konzernprivilegierung** vorsieht, die an die DSGVO anknüpft (Art. 4 Nr. 19) vorteilhaft und sinnvoll sein, wenn die Öffnung von Beschäftigtendaten gegenüber mehreren verantwortlichen Stellen im Konzern durch Sicherungen kompensiert wird und klare Verantwortlichkeiten festgelegt werden.

4 Politisch bestimmbare Rahmenbedingungen

Eine adäquate Gesetzgebung ist die Grundlage für eine Verbesserung des Datenschutzes in einer sich immer mehr digitalisierenden Arbeitswelt. Das Heil des Persönlichkeitsschutzes für Beschäftigte kann nicht ausschließlich in der Gesetzgebung liegen. Vielmehr müssen in den Betrieben, Branchenverbänden, Gewerkschaften, Beschäftigtenvertretungen, Aufsichtsbehörden und bei den Anbietern von IKT-Lösungen Konzepte für einen datenschutzkonformen IKT-Einsatz am Arbeitsplatz erforscht, diskutiert, entwickelt und implementiert werden. Hierfür kann als Instrument der politischen Planung die Einrichtung eines **Datenschutzbeirats im Bundesarbeitsministerium** sinnvoll sein. Dieser kann Vorschläge für überbetriebliche Vereinbarungen machen oder diese gar verbindlich initiieren.

Bisher erfolgen öffentlich geförderte **Forschungs- und Entwicklungsanstrengungen** im Bereich des Datenschutzes zumeist jenseits des betrieblichen Anwendungsfeldes. Dies muss sich angesichts der neuen Herausforderungen durch Anwendungen in den Bereichen Industrie 4.0 und Big Data ändern. Bisher laufen Forschungs- und Entwicklungsarbeiten auf Initiative von IKT-Anbietern und Arbeitgebern insbesondere darauf hinaus, die Beschäftigtenüberwachung zu perfektionieren. Dem sind Anstrengungen für ein Mehr an Persönlichkeitsschutz entgegenzusetzen, die staatlich gefördert werden.

5 Abschließende Bemerkungen

IKT hat große **positive Auswirkungen** auf die Arbeitswelt. Sie führt zu Produktivitätssteigerungen und kann, sinnvoll eingesetzt, dazu beitragen, den Arbeitnehmern ihre Tätigkeit zu erleichtern, sie zu qualifizieren und ihren Arbeitsplatz zu sichern. Der Einsatz von IKT kann zu einer erhöhten Zufriedenheit bei den Beschäftigten führen, etwa, wenn Kreativität gefördert wird, die Arbeitsleistungen besser sichtbar werden oder spielerische und Team-Elemente bei der Arbeit einfließen. Arbeitnehmervertretungen sollten deshalb die Einführung derartiger Systeme grundsätzlich fördern und fordern.

Es sollte jedoch allen Seiten, auch den Arbeitnehmervertretungen und den Beschäftigten, vermittelt werden, dass die Attraktivität von IKT-Systemen eine persönlichkeitsgefährdende Kehrseite hat. Arbeitgeber betonen gerne die mit IKT verbundenen Verbesserungen für ihre Beschäftigten, verschweigen jedoch die damit verbundenen zusätzlichen Überwachungs- und Kontrollmöglichkeiten. Diese Möglichkeiten sind jedoch oft der eigentliche Grund für die Einführung bestimmter Systeme. Ein solcher Einsatz führt zu einer schleichenden Entmündigung der Betroffenen. Diese ist nicht nur persönlich eine Gefahr für die Betroffenen, sondern auch für jede demokratische Gesellschaft, deren Grundlage mündige, **meinungsfreudige und kreative Menschen** sind. Der Persönlichkeitsschutz von Beschäftigten sollte daher letztlich das ureigene Interesse der Unternehmensleitungen sein. In einem Klima der Überwachung und der Kontrolle werden Kreativität, Motivation

und Produktivität beeinträchtigt, die aber andererseits Voraussetzung für wirtschaftlichen Erfolg sind.

Deshalb sollte und kann das Anliegen eines modernen Beschäftigtendatenschutzes nicht länger durch sehr allgemein gehaltene Regelungen erfüllt und die Auslegung den Arbeitsgerichten überlassen werden. Es muss – insbesondere nachdem Europa den Rahmen gesteckt hat – auch ein Anliegen des nationalen Gesetzgebers sowie der Vertretungen von Beschäftigten und Arbeitgebern sein. Der Deutsche Gewerkschaftsbund (DGB) hat, nachdem über den Text der DSGVO Einvernehmen erzielt worden war, signalisiert, dass er die Ausarbeitung eines nationalen Beschäftigtendatenschutzgesetzes fordert und dass er sich an dessen Ausarbeitung konstruktiv beteiligen will. Die Diskussion über ein **modernes Beschäftigtendatenschutzgesetz** muss heute und mit hoher Priorität geführt und zu einem Erfolg gebracht werden.

Monika Heim

Persönlichkeitsrechte werden nicht am Werkstor abgegeben!

Überlegungen einer Betriebsrätin zu einem wirkungsvollen Beschäftigtendatenschutzgesetz

Beschäftigtendatenschutz – eine never ending story. In den vergangenen Jahren, wurde das Thema von den unterschiedlichsten Regierungskoalitionen aufgegriffen, zuletzt Anfang 2013. Es wurde geredet, festgestellt, dass unbedingt eine gesetzliche Regelung notwendig sei, manche Entwürfe wurden erstellt, alle wurden letztendlich verworfen – zum Glück, möchte man sagen.

Aus meiner Sicht waren die Entwürfe der jeweiligen Regierungsparteien zum Nachteil der Beschäftigten. Die Wünsche der Arbeitgeber waren stets höher gewichtet, ein Ausgleich fand meist nur sehr bedingt statt.

Videoüberwachung zum Beispiel wurde immer als notwendige Maßnahme akzeptiert. Der Schutz des Eigentums wog gegenüber dem Persönlichkeitsrecht der Beschäftigten immer schwerer.

Sehr auffällig war vor allem eines: Die Betroffenen wurden nicht befragt. Juristen, insbesondere aus den Reihen der Politik und Spitzenfunktionäre der Arbeitgeberverbände unterhielten sich darüber, was im Beschäftigtenverhältnis an Überwachung zumutbar sei und was nicht. Wenige GewerkschafterInnen und noch weniger BetriebsrätInnen wurden in die Überlegungen einbezogen, auch Ideen von DatenschützerInnen fanden merkwürdigerweise nur wenig Resonanz (wenngleich wir uns 2013 beim letzten Versuch einer Regierung, ein Beschäftigtendatenschutzgesetz auf den Weg zu bringen, auch ungefragt massiv einmischten).

Regelungsinhalte

Vorausschicken möchte ich eines: Ein Unternehmen, ein Chef soll kontrollieren dürfen, ob seine Beschäftigten die geforderte Arbeitsleistung erbringen oder ob sie das Unternehmen schädigen. Den Ansatz allerdings, jedem Beschäftigten generell Betrugsabsicht zu unterstellen und dies mit Hilfe moderner Überwachungsmethoden verhindern zu wollen, halte ich für grundsätzlich falsch. Kontrolle kann auch stattfinden durch Präsenz und Gespräche. Eine Führungskraft, die Login-Zeiten kontrolliert statt Arbeitsergebnisse, die Algorithmen die Beurteilung ihrer Leute überlässt, zeigt letztlich nur eines: Führungsschwäche.

Das geht gar nicht!

- Bewerbung: Fragen nach Schwangerschaft, Ermittlungsverfahren, Behinderungen, das Nutzen von Suchmaschinen oder Erkundigungen beim aktuellen oder vorigen Arbeitgeber
- Einstellung: Bluttests, psychologische Test, ärztliche Untersuchungen, wenn das Stellenprofil dies nicht zwingend erfordert
- Anlasslose Screenings (Deutsche Bahn, Telekom), Massenscreenings aus vorgeblichen Compliance-Gründen, Verwendung von Zufallsfunden anderer Art bei begründeten Screenings
- Einsatz von IT-gestützten Überwachungsmaßnahmen bei nur vermutetem Fehlverhalten einer Beschäftigten, besonders in Bezug auf Bagatelldelikte
- Heimliche Überwachung, generelle offene Videoüberwachung
- Allgemeine Persönlichkeitsprofile
- Aufzeichnung von Telefongesprächen ohne festgeschriebene Löschfristen
- Ein Konzernprivileg, insbesondere dann, wenn sich Konzernteile außerhalb der Europäischen Union befinden
- Struktur und Sprache wie im letzten Entwurf von 2013, die auch Juristen verzweifeln ließen

Ein Beschäftigtendatenschutzgesetz muss als Prämisse haben, die Persönlichkeitsrechte von Beschäftigten zu wahren. Was braucht es dazu?

- Wer nicht hören will, muss zahlen! Festgeschrieben werden muss vor al-

lem eines: Ein Beweisverwertungsverbot von unrechtmäßig erhobenen Daten verbunden mit einer empfindlichen Geldstrafe. Verstöße gegen den Datenschutz müssen wehtun.

- Es kann nur einen geben!?
  Besonders in großen Betrieben leiden betriebliche Datenschutzbeauftragte (bDSB) unter einer hohen Arbeitsbelastung. Zudem kennen sie sich mit den Abläufen oft nicht in der erforderlichen Detailtiefe aus. Die Bestellung von geschulten „DatenschutzkoordinatorInnen“ in größeren oder besonders sensiblen Bereichen wie etwa Personalverwaltung oder Betriebsrat, die dem bDSB zuarbeiten, sorgt dafür, dass Vorabkontrollen und Prüfungen kenntnisreicher und effektiver ablaufen. Als Beispiel mag hier die Funktion der Sicherheitsbeauftragten aus den Arbeitsschutzgesetzen dienen.
- Nein!
  Betriebliche Datenschutzbeauftragte müssen ein Vetorecht haben, das sich im Zweifel auch gerichtlich durchsetzen lässt. Das ist besonders in Betrieben wichtig, wo kein Betriebsrat bei Verstößen gegen das Beschäftigtendatenschutzgesetz Klage beim Arbeitsgericht erheben kann.
- Gesamtschau / „Technologiefolgenabschätzung“
  Das Unternehmen muss gemeinsam mit dem bDSB und – falls vorhanden – dem Betriebsrat regelmäßig die Summe aller eingesetzten Verfahren, die mittelbar oder unmittelbar der Leistungs- und Verhaltenskontrolle dienen können, prüfen. Die Prüfung auf eine einzelne Kamera zum Beispiel mag ergeben, dass deren Einsatz notwendig und sinnvoll scheint. Sind allerdings schon viele Kameras in unterschiedlichen Bereichen (jede einzeln betrachtet sinnvoll und notwendig) im Einsatz, mag sich ein anderes Bild ergeben.
- Pflicht zu Schulungen
  Nicht nur der bDSB soll sich regelmäßig fortbilden, auch für die Beschäftigten, ganz besonders für die Führungskräfte aller Ebenen, halte ich Pflichtschulungen, die regelmäßig wiederholt werden, für notwendig. Manches Mal, so meine Erfahrung, kommt der Wunsch nach Überwachung auch aus den Reihen der KollegInnen. Sensibilisierung hier kann auch zu einem besseren Verständnis von Datenschutz allgemein führen.
- Zwingende Konsultation des Betriebsrates
  Datenschutzbeauftragte sollen prüfen, ob ein Verfahren Leistungs- und Verhaltenskontrolle ermöglicht. Mitunter gibt es zu diesem Punkt unterschiedliche Sichtweisen (immerhin wird ein bDSB vom Unternehmen bestellt und kann aus Sicht eines Betriebsrates auf der Unternehmerseite stehen). Insofern sollte ein Verfahren erst dann als erlaubt gelten, wenn sowohl bDSB als auch Betriebsrat ihre Zustimmung gegeben haben. Das Recht des Betriebsrates ergibt sich zwar schon aus dem Betriebsverfassungsgesetz, gut wäre aber ein entsprechender Passus auch im Beschäftigtendatenschutzgesetz.
- Ausweitung und Sicherstellung der personellen Kapazitäten in den Datenschutzbehörden
  Die Aufsichtsbehörden sind chronisch unterbesetzt und können ihren Kontrollpflichten nur schwer nachkommen. Wünschenswert ist daher, dass in einem Beschäftigtendatenschutzgesetz auch diesem Aspekt Rechnung getragen wird.
- Privacy by Design
  Bevorzugung von Software, die (Beschäftigten-)Datenschutz bereits eingebaut hat. Bisher ist es ja häufig so, dass eine Software mehr kann als ursprünglich benötigt wird. Vor allem Standardsoftware soll vielen Einsatzszenarien gerecht werden können. Meist wird das Programm erst nach der Installation mit Rollen und Berechtigungen versehen. Es ist alles erlaubt und wird erst später Schritt für Schritt eingeschränkt. Das bringt manchen Arbeitgeber erst auf die Idee, man könnte doch...
- Freiwillige Transparenz und Auskunftspflicht zu erhobenen und gespeicherten Daten, ebenso zu den verwendeten Verfahren, insbesondere dann, wenn staatliche Stellen Auskünfte über den / die Beschäftigte nachfragen.
- Recht auf Verschlüsselungstechniken auch im innerbetrieblichen Mailverkehr
- Pflicht zum verschlüsselten Datentransfer zwischen Betrieb und externen Empfängern. Besonderer Schutz bei der elektronischen Kommunikation rings um Finanzen, Gesundheit, Versicherungen, etc.
- Beschwerdemöglichkeiten für Beschäftigte
- In aller Regel sind Beschäftigte verpflichtet, ihre Beschwerden intern zu melden. Dafür gibt es den Betriebsrat, das Personalwesen, den bDSB und vielleicht eine Compliance-Stelle. Was aber, wenn den Beschwerden dort nicht nachgegangen wird? Im Gesetz sollte daher das Recht auf Beschwerde ohne Nachteile außerhalb der eigenen Firma festgeschrieben sein.

Zusätzlich zu Regelungen der weiter oben angesprochenen Punkte

- Regelung zu Kontrolle der elektronischen Personalakten
- Regelungen zu Cloud-Diensten, Big Data, Festschreibung eines persönliches Rechts auf Verarbeitung im europäischen Raum
- Eine Formulierung, die auch zukünftige Technologien mit einschließt und dem Schutzgedanken Rechnung trägt.

Alles nur Träume?

Ihnen mögen diese Überlegungen utopisch, als ein „Wünsch Dir was“ erscheinen, fernab jeglicher Realität.

Nun, es wird tatsächlich schwierig zu verhandeln und durchzusetzen sein. Legen wir aber einen Entwurf vor, der bereits Arbeitgeberinteressen berücksichtigt, so wird unweigerlich ein Kompromiss eines Kompromisses gefunden. Die politischen Abstimmungsprozesse der Vergangenheit zum Beschäftigtendatenschutz belegen dies eindrucksvoll.

In der Abwägung zwischen wirtschaftlichen Interessen und Persönlichkeitsrechten der Beschäftigten muss der Mensch Vorrang haben – kompromisslos.

Wir haben 2013 gelernt, dass Proteste wirksam und erfolgreich sein können. Wichtig wird sein, dass unsere politischen Bündnispartner uns schnell alarmieren, sobald der erste Entwurf bekannt wird. Auch die Gewerkschaften sind in der Pflicht zu informieren, denn sie werden im Rahmen von Konsultationen ebenfalls relativ früh in das Gesetzgebungsverfahren eingebunden. Es sollen nicht nur unsere Funktionäre

mitreden dürfen, sondern auch wir Beschäftigte und Betriebsräte. Schließlich sind wir die Betroffenen.

(Wirksamer Beschäftigtendatenschutz könnte ja auch zu einer Tarifforderung erhoben werden…)

Aktive, an Datenschutz allgemein und dem Beschäftigtendatenschutz im Besonderen interessierte Menschen können gemeinsam mit unseren Interessensvertretern in Betrieben, Gewerkschaften, Datenschutzverbänden, Politik und der Zivilgesellschaft ein Beschäftigtendatenschutzgesetz erwirken, das seinen Namen zu Recht trägt.

Packen wir's an.

Lothar Schröder

Zur Statik des Beschäftigtendatenschutzes

Elisha Graves Otis wird nachgesagt 1856 in den Vereinigten Staaten den Aufzug erfunden zu haben. Seinen Namen lesen wir als Firmenbezeichnung heute noch in vielen Aufzügen, auch hierzulande. Was hat er getan? Er hat Hebebühnen, Motoren, Stahlseile und Metallkonstruktionen zusammengefügt – all dies gab es vorher schon. Seine Neukombination erlaubte es viel höher zu bauen, herkömmliche Dimensionen wurden entgrenzt. Das hat unsere Architektur weltweit und schließlich auch unser urbanes Leben gravierend verändert.

Heute kombiniert die Digitalisierung jene Elemente neu, aus denen unsere Arbeitswelt gebaut ist. Herkömmliche Bindung in Ort und Zeit wird entgrenzt. Es entsteht eine neue Architektur für die Arbeit der Zukunft. Darüber besteht Anlass festzulegen, welche Statik diese Arbeitswelt haben soll und auf welche Fundamente wir den Schutz der Persönlichkeitsrechte der darin arbeitenden Menschen künftig bauen wollen.

Den Schutz der Persönlichkeitsrechte im Betrieb den vermeintlichen Wirtschaftsvorteilen der heutigen Grenzenlosigkeit zu opfern und Schutzvorschriften zu deregulieren wäre reichlich kurzsichtig. Genauso hätte die Architektenkammer des Staates New York im Jahr 1856 gehandelt, wenn sie damals festgestellt hätte: Jetzt, da man sehr viel höher bauen kann, gilt es Bauvorschriften zu deregulieren, feuerpolizeiliche Auflagen abzuschaffen, den Statikern ihre Rolle abzusprechen und auf Sicherheit am Bau zu verzichten. Wäre einem derart imaginären Aufruf gefolgt worden, sähen Manhattan und andere Großstädte heute wohl anders aus.

Weil die Architektur der Arbeitswelt sich ändert und sich wohl in Zukunft noch dynamischer und gravierender ändern wird, brauchen wir Sicherheitsvorschriften und Gewährleistungsinstrumente für den Schutz der Beschäftigtendaten. Ein Beschäftigungsdatenschutzgesetz muss – im übertragenen Sinne – die grundlegende Bauvorschrift für den Schutz der Persönlichkeitsrechte werden. Auch ein Blick in die jüngere Historie macht deutlich, dass ein derartiges Werk für den Schutz von Beschäftigtendaten längst überfällig ist.

Die Datenschutzbeauftragten des Bundes und der Länder fordern schon seit 1984 spezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. In ihrer 43. Konferenz haben sie 1992 die Politik an dieses Anliegen erinnert und Normen gefordert, die schon damals weitsichtig waren. Es ging ihnen darum, die Erstellung von Persönlichkeitsprofilen für unzulässig zu erklären, Personalauswahlentscheidungen nicht allein auf Informationen zu stützen, die unmittelbar durch Datenverarbeitung gewonnen werden und Datenübermittlung ins Ausland nur dort zuzulassen, wo ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist.

Nun schafft die europäische Datenschutzgrundverordnung einen Rechtsrahmen, der einheitliche Bedingungen für den Datenschutz in den Ländern der europäischen Gemeinschaft schafft. Gerade im Beschäftigtendatenschutz lässt der Paragraph 88 aber spezifische nationale Regelungen zu und geht sogar soweit, kollektive Normen über Tarifverträge und Betriebsvereinbarungen als Spezialregelungen zu unterstützen. Wer also seit 1984 darauf gewartet hat, dass ein umfassendes und feinziseliertes Datenschutzrecht alle Fragen, die sich zum Schutz der Persönlichkeitsrechte im Betrieb gestellt haben, ein für alle Mal möglichst europaweit einheitlich beantwortet, muss enttäuscht sein. Weitere Gestaltungsanstrengungen sind notwendig und sie müssen sich Bedingungen annehmen, die sich seit dem Orwell-Jahr verändert haben.

Zu der Zeit, als der erste Ruf nach einem Beschäftigtendatenschutzgesetz entstand, machten Betriebsräte schon Erfahrungen mit der Ausgestaltung des Paragraphen 87 Abs. 1 Nr. 6, einer Rechtsvorschrift, die Mitbestimmung bei der Einführung und Anwendung technischer Einrichtungen gibt, die eine Leistungs- und Verhaltenskontrolle bei den Beschäftigten ermöglichen. Damals begegnete uns der Computer noch als Automat, in Form von Stechuhren und lochkartengesteuerter Großrechnersysteme. Der Computer wurde in den 80ern zum Werkzeug, als die PCs auf den Schreibtischen ihren Platz fanden. Gleichzeitig verbreiteten sich ergebnisorientierte Arbeitsformen und verbreitete sich die Kennzahlensteuerung in den Betrieben immer mehr. Längst sind Rechner zum Medium geworden. Mit Laptops und Smartphones ausgerüstet arbeiten wir in Zügen, auf

Flughäfen und überall dort, wo ein akzeptabler Netzzugang existiert. Heute erscheinen uns Rechnersysteme als Plattformen, die Arbeit vermitteln und eine digitale Reputation abverlangen. Wir tragen Smartphones und Wearables ständig bei uns und das allgegenwärtige maschinelle Wirken erzeugt Datenschatten, oft ohne unser Zutun und Wissen. Daneben ist der Rechner dabei, zum Propheten zu mutieren. Aus den Daten der Gegenwart und der Vergangenheit, auch der Berufstätigen, können Prognosen über das Verhalten in der Zukunft ableitet werden. BigData ist der Sammelbegriff für eine analytische Datenauswertung, die sich in Dimension, Geschwindigkeit und Umfang des Datenzugriffs von herkömmlichen Möglichkeiten unterscheidet.

Das trifft auf eine veränderte Wahrnehmung in unserer Gesellschaft. Datenauswertungen haben den Ruf des Objektiven erobert. Was zählbar ist, zählt und gezählt wird, was sich rechnet. Betriebsräte kennen längst die Auswirkungen einer Totalisierung des Zählbaren. Benchmarkingsysteme haben über die Zeit in die Betriebe Einzug gehalten. Sie vermitteln vermeintliche Objektivität und meistens Anpassungsdruck, im ungünstigsten Fall bis zum Individuum.

In der herkömmlichen Arbeitswelt fanden Hierarchiekonflikte um Zeit, Raum der Arbeitsverrichtung und um Entlohnungsbedingungen statt. In der Zukunft werden Herrschaftskonflikte auch um Daten geführt werden. Nicht alles Zählbare muss gezählt, nicht alles Digitalisierbare muss digitalisiert, nicht alles Durchschaubare muss transparent gemacht werden. Die Digitalisierung kann zwar dabei helfen unsere Arbeitswelt intelligenter zu machen, sie wirkt aber nicht per se humanisierend. Und auf alle Fälle stellt sie neue Herausforderungen für den Schutz der Persönlichkeitsrechte.

Datenschützer stellen seit jeher den Schutz der Person und seiner Rechte – die Persönlichkeitsrechte – in den Mittelpunkt ihres Wirkens. Persönlichkeiten drücken sich aber nicht allein in der Fülle der über sie verfügbaren, ökonomischen Daten aus. Der Mensch hat Glaube, Mitgefühl, Intuition, Scham, Verantwortungsbewusstsein, Launen, Ideologie und Unzulänglichkeiten – das macht den Menschen aus. All das ist mehr, als eine Kenngröße in einem Performancebenchmark. Digitale Reputationen können den Menschen in seinem Wesen nicht angemessen abbilden und Algorithmen erlauben deswegen keine Entscheidungen auf Basis vollständiger Information. Ihnen fehlt auch ein wesentliches Element des Menschen, dessen Bewusstsein mit einem Gefühl für Recht und Unrecht. So wenig wie ein Bruttosozialprodukt erschöpfend den Wohlstand eines Landes beschreiben kann, so wenig kann die Masse von Kennziffern in den Betrieben universell über das Menschliche Auskunft geben und der Vielfalt unterschiedlicher Persönlichkeiten gerecht werden. Gleichzeitig betont unsere Gesellschaft, dass die Wirtschaft den Menschen zu dienen habe und nicht umgekehrt und belohnt gleichwohl das Datensammeln als Geschäftszweck an sich. Innerhalb kürzester Zeit sind mit Firmen wie Google, Facebook und mit den Applikationen wie WhatsApp, Airbnb und Uber Datenoligarchien mit gewaltigem Marktwert entstanden, die hinsichtlich der Persönlichkeitsrechte ein offensichtlich anderes Menschenbild haben, als jenes, das handlungsleitend für deutsche Datenschützer über Jahrzehnte hinweg war. Trotzdem nutzen wir die Angebote, wir sind heute Teil des Problems. Unser Kundeninteresse ringt mit dem Interesse die Persönlichkeitsrechte zu schützen. Der Kunde in uns will wissen, wo sich das Paket gerade befindet, der Beschäftigte in uns verwahrt sich gegen Tracking-Systeme.

Erst Skandale rütteln auf und der Schutz unserer Daten wird uns wichtiger. Unsere Gesellschaft geht mit den Persönlichkeitsrechten um, wie viele von uns mit der eigenen Gesundheit: Erst wenn sie nicht mehr vorhanden ist, merken wir, wie wichtig sie ist und versprechen uns künftig sorgfältiger mit uns selbst umzugehen. Beim Datenschutz machen die großen Missbrauchsfälle deutlich, was der Schutz der Persönlichkeitsrechte ausmacht. Wir erinnern uns an das Screening bei der Bahn, die Bespitzelung bei der Telekom, um Videoüberwachung bei LIDL, Detektiveinsätze bei Schlecker, Krankendatensammlung bei der Post, die Entrüstung um die Bespitzelungsprodukte diverser Spitzelsoftwareanbieter. Diesen Ereignissen gemeinsam ist ein öffentliches Aufbegehren mit einer kurzen Halbwertszeit, das sich selten in konkrete kontinuierliche Gestaltungsarbeit übersetzt hat. Solche Anstrengungen begründen sich aber schon aus dem Alltäglichen, dem Unskandalösen, dem Nachlesbaren.

„Ohne Internet wäre es richtig schwer gewesen, jemanden zu finden, 10 Minuten für sich arbeiten zu lassen und dann zu feuern. Aber jetzt mit der Technologie findet man sie, zahlt ihnen winzige Geldbeträge und wird sie los, wenn man sie nicht mehr braucht.“ Mit diesem Zitat beschreibt Lukas Biewald, der Vorstandsvorsitzende von Croudflower die Möglichkeit des Croudsourcing. Darin wird deutlich, wie wenig sich manche Protagonisten einer veränderten Arbeitswelt der sozialen Verantwortung stellen. Wir sollten nicht annehmen, dass derartige Entscheidungsträger mit dem Schutz der Persönlichkeitsrechte rücksichtsvoller sind und wir sollten nicht glauben, dass eine digitale Reputation, die den Crowdsourcees abverlangt wird, ohne Sogwirkung für herkömmliche Beschäftigte bleibt. Längst vermischt sich im Erwerbsleben Privates und Berufliches. Die Grenzlinie zwischen Arbeit und Freizeit erodiert. Da wird schon mal der Wunsch eines Arbeitnehmers auf Einrichtung eines Telearbeitsplatzes arbeitgeberseitig abgelehnt, weil für den Arbeitgeber die Urlaubsbilder des Beschäftigten nicht auf Einschränkungen in dessen Mobilität hindeuten. Da wird natürlich der Bewerber gegoogelt, obgleich das Netz auch Datensammlungen zu Tage fördert, die nicht beim Betroffenen erhoben wurden.

Ein Ungleichgewicht hat sich jedoch über die Jahrzehnte hinweg nicht verändert. Die Arbeitnehmer stehen im Beschäftigungsverhältnis den Arbeitgebern als die tendenziell Schwächeren gegenüber. Deswegen darf ihnen auch keine universelle Einwilligung zur jedweden Datenerhebung abverlangt werden. In diesen und anderen Fragen braucht die europäische Datenschutzgrundverordnung eine spezifische Ausgestaltung, die dem Wesen des deutschen Arbeitsrechts in unserer Kultur gerecht wird. Einwilligungen müssen begrenzt und nur befristet gültig sein. Wir bräuchten ein System von Verfallsdatum und Gütesiegel für guten Datenschutz, dies hat bereits die Enquete-Kommission „Internet und digitale Gesellschaft“ empfohlen. In einem Minderheitenvotum wurden zahlreiche Anliegen der Gewerkschaften zum Arbeits-

nehmerdatenschutz aufgegriffen. Gefordert wird hiernach ein eigenständiger, gesetzlicher Rahmen, der die Persönlichkeitsrechte von Berufstätigen schützt. Es geht darum, Generaleinwilligungen zur Datenerhebung und -nutzung zu verbieten, anlasslose Beobachtung und Überwachung einzugrenzen, Kunden- von Beschäftigtendaten zu trennen und die Position der betrieblichen Datenschutzbeauftragten zu stärken. Gewerkschaften sind sich mit den Oppositionsparteien im Bundestag einig, dass die Mitbestimmungsrechte gestärkt werden müssen, um in den Betrieben auf einer zeitgemäßen Statik für die veränderte Architektur der Arbeitswelt aufbauen zu können.

Dort geht es längst nicht mehr nur um Leistungs- oder Verhaltenskontrollen durch betriebliche Systeme. Es geht um private Vorlieben, Kontakte, Leidenschaften und Einstellungen von Beschäftigten, die über eine Netzrecherche zu Tage gefördert werden können. Mit einem umfassenden Mitbestimmungsrecht zum Schutz der Persönlichkeitsrechte müssen Betriebsräte die betriebliche Nutzung derartiger Informationen reglementieren können. Die Oppositionsparteien machten darüber hinaus in der Enquete-Kommission deutlich: Wir brauchen einen Immunitätsschutz für Betriebs- und Aufsichtsräte ebenso wie ein Verbandsklagerecht und wirksame Sanktionsklauseln, die jene Betriebe treffen, die Persönlichkeitsrechte verletzten. Für die im Deutschen Gewerkschaftsbund zusammengeschlossenen Gewerkschaften ist es darüber hinaus notwendig Beweisverwertungsverbote für unzulässig erhobene Daten gesetzlich zu normieren und ein Reglement für Screenings und biometrische Kontrollen zu schaffen. Das Fragerecht der Arbeitgeber bei Einstellungen soll ebenso begrenzt werden, wie die Datenerhebung mittels ärztlicher Untersuchungen von Nachwuchskräften.

Nach mehr als 30 Jahren ohne Beschäftigtendatenschutzgesetz und angesichts der Rasanz der gegenwärtigen Entwicklung ist jedoch kritisch danach zu fragen: Lässt sich heute mit einem Beschäftigtendatenschutzgesetz ein Regelwerk schaffen, das dauerhaft alle Aspekte der Bedrohung von Persönlichkeitsrechten minimiert?

Viele Kommentatoren der Digitalisierung verbinden Prognosen zur weiteren Entwicklung mit den Begriffen „exponentielle Wirkung“, „Neukombinatorik“, „Prozessmusterwechsel“ und „Disruption“. Wenn sich die Dynamik und die Dimension der Digitalisierung tatsächlich nur zum Teil entlang dieser Bezeichnungen entwickelt, braucht der Schutz der Persönlichkeitsrechte Mechanismen, die die gesetzgeberische Grundlage flankieren. Die grundlegenden Architekturvorschriften für die Digitalisierung der Arbeitswelt brauchen Garantensysteme und Reaktionsmechanismen, die der Veränderung Rechnung tragen:

1. Die Deutsche Bahn und die Deutsche Telekom haben aus ihren Datenschutzskandalen Konsequenzen gezogen. Sie haben jeweils einen Datenschutzbeirat eingerichtet, der das Datenschutzverhalten der Unternehmen kritisch begleitet. Die Datenschutzexperten im Beirat der Telekom beraten das Unternehmen bei neuen Produktlinien, der Datenschutzorganisation aber auch zu ethischen Prinzipien für den Schutz der Persönlichkeitsrechte. Ein entsprechender Datenschutzbeirat beim Bundesarbeitsministerium könnte dabei helfen, den Gesetzgeber zu den dynamischen Veränderungen in Technik und Wirtschaft auf der Höhe der Zeit zu beraten, spezifische deutsche Rechtsnormen empfehlen, gute Gestaltungsbeispiele der Arbeitswelt der Zukunft zum Austausch bringen und in ministeriellem Auftrag öffentlich bekanntgewordenen Datenschutzverstößen nachgehen.

2. In den 90er Jahren hat die Deutsche Postgewerkschaft ein bemerkenswertes Datenschutzprojekt durchgeführt. Experten aus verschiedenen gesellschaftlichen Gruppen arbeiteten daran mit quid! zu entwickeln. Quid! steht für „Qualität im Datenschutz“ und war als Qualitätszeichen für gutes betriebliches Verhalten im Datenschutz gedacht. Der Dialog verschiedener Interessengruppen war damals erfolgreich und ist heute notwendiger denn je. Ein Indikatorenmodell für Arbeitnehmerdatenschutz wird heute dringend benötigt.

   Wenn Betriebe nach Benchmarks gesteuert werden, sollten Benchmarksysteme für Arbeitnehmerdatenschutz gefördert werden. Wenn es der DGB Index Gute Arbeit geschafft hat, sich zum landesweit anerkannten Indikatorenmodell zum Thema „Gute Arbeit“ zu entwickeln, dann müsste es möglich sein, ein entsprechendes Modell für Arbeitnehmerdatenschutz zu schaffen. Ein Indikatorenmodell kann das betriebliche Verhalten im Arbeitnehmerdatenschutz unterschiedlicher Betriebsteile aber unterschiedlicher Branchen vergleichen, Handlungsbedarfe in Teilaspekten erkennbar machen und für die Gestaltungsarbeit im Betrieb eine übergreifende Vergleichsbasis verschaffen.

3. Daneben sollten wir darüber nachdenken, mit welchen Mechanismen wir den Glauben erschüttern können, dass alles, was in Daten ausgedrückt ist, auch den Ruf der Objektivität und Unfehlbarkeit verdient. Maschinen werden von Menschen programmiert und die sind ebenso fehlbar, wie Algorithmen selbst die Realität verzerren können. Um Leben und Gesundheit zu schützen werden Hersteller von Produkten in Deutschland mit Produkthaftung in die Pflicht genommen – sie haften im Falle von fehlerhaften Erzeugnissen gegenüber dem Nutzer für Schäden, die durch die Produkte entstehen. Wir sollten darüber nachdenken, ob wir Big-Data-Auswertungen nicht ebenfalls als Produkte betrachten, für die deren Erzeuger im Schadensfall zu haften haben. Dieses Recht könnte uns etwas dabei helfen, Verantwortung dort zu manifestieren, wo Ertrag aus Daten entsteht, die oft für ganze andere Zwecke erhoben wurden.

4. Mit etwas Schmunzeln sei abschließend angeregt, in deutschen Betrieben Datenauswertungen die entscheidend die Arbeitsbedingungen prägen sollen, nur noch mit einem Disclaimer zuzulassen, der den Mechanismus aufgreift, den wir längst von der Medikamentenwerbung kennen. Danach dürften Benchmarks nur verpowerpointet werden, wenn auf ihnen zugleich steht: „Zu Risiken und Nebenwirkungen lesen Sie den Programmcode und fragen Sie Ihre Datenanalytiker oder Programmierer.“

Neil Watkins

Transatlantic Compliance: Understanding today's picture and best practice next steps

A complicated picture just got more complex. The transatlantic transfer of personal data between the European Union and the United States is now governed by new data privacy compliance obligations following an October 2015 ruling that invalidated the previous Safe Harbour privacy accord. This applies to personal data, including employee data, collected in the EU by a branch or a business partner of a United States-based company which receives the data and then uses it in the United States.[1] For businesses, this means a new set of rules to learn and a new set of standards to adhere to.

The background to this latest development can be traced back to 1995 and the establishment of the EU Data Protection Directive (Directive 95/46/EC). This Directive was enacted to balance the protections for individuals' privacy with the free movement of personal data within the European Union. The Directive established limits regarding the collection and use of personal data and required that each Member State establish an independent national body to supervise activities associated with the processing of personal data.

Among other things, the Directive stipulates that personal data may only be transferred from a Member State to a "third country" (e.g. those outside the EU) if that country provides an adequate level of protection, subject to certain exceptions. The Article 29 Data Protection Working Party (the "Article 29 Working Party"), established pursuant to the Directive, negotiated with U.S. representatives regarding the protection of personal data transferred between the EU and U.S. and, as a result, the Safe Harbour Principles were issued by the U.S. Department of Commerce in July 2000.

Turbulence under Safe Harbour

In the years after its inception, Safe Harbour became subject to criticism. The criticism focused on the ability of U.S. companies to "self-certify" under the program, and that the Federal Trade Commission (FTC) which policed Safe Harbour was not suitably stringent. Indeed, controversy over Safe Harbour had been brewing for years, not least following Edward Snowden's (a former NSA contractor) whistle-blowing revelations which caused the European Commission to call for a review of the program. Then, a landmark ruling in October 2015 impacted the entire compliance landscape. In the case of Schrems v. Data Protection Commissioner, the European Court of Justice ("ECJ") invalidated the Safe Harbour framework. This effectively meant that personal data transferred from

Members States in Europe to the U.S. pursuant to Safe Harbour was no longer deemed to be adequately protected, a decision that left the nearly 4,500 companies that self-certified under Safe Harbour in a state of flux.

In fact, efforts to update and replace Safe Harbour with a "2.0 version" had been underway for some time, but the Schrems ruling demanded an urgent response. EU data protection authorities (gathered together as the Article 29 Working Party) set a 31 January 2016 deadline to replace the invalidated mechanism and for the EU and the U.S. Department of Commerce to develop a new solution.

The Introduction of the EU-U.S. Privacy Shield

On 2 February 2016, the European Commission and the U.S. Department of Commerce reached a deal on a new transatlantic personal data transfer pact, the resulting EU-U.S. Privacy Shield. On 12 July 2016, the European Union Commission officially adopted the EU-U.S. Privacy Shield (see http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf and https://www.commerce.gov/privacyshield), representing the culmination of a long process to address the shortcomings of the EU-U.S. Safe Harbour framework which was invalidated in October 2015 by the ECJ. This follows the approval of Privacy Shield on 8 July 2016 by the Article 31 Committee (originally established under the Directive 95/46/EC), which includes representatives of the EU Member States. While the European Union Commission's adequacy decision is immediately effective, U.S.-based companies will be given until 1 August 2016 to review the new framework's requirements before being able to register and self-certify their compliance with Privacy Shield. For those U.S.-based companies that do register in August and September 2016, these companies will be able to take advantage of a nine-month "grace period" (i.e., through April 2017) to address their compliance-related requirements with third parties relative to adherence with the new framework.

The European Commission has proposed that the new Privacy Shield framework be deemed adequate to enable transfers of personal data between EU Member States (and presumably the three European Economic Area members, i.e., Iceland, Liechtenstein and Norway) and the United States. The adequacy decision by the Commission, however, does state the following:

"The EEA Joint Committee has to decide on the incorporation of the present decision into the EEA Agreement. Once the present decision applies to Iceland, Liechtenstein and Norway, the EU-U.S. Privacy Shield will also cover these three countries and references in the Privacy Shield package to the EU and its Member States shall be read as including Iceland, Liechtenstein and Norway."

The Privacy Shield framework is described by the U.S. Department of Commerce to embody "a renewed commitment to privacy by the U.S. and the EU, and to ensure it remains a living framework subject to active supervision, the Department of Commerce, the FTC and EU DPAs [Data Protection Authorities] will hold annual review meetings to discuss the functioning of and compliance with the Privacy Shield." (See https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield.)

The stated aim is to strengthen cooperation between the FTC and EU DPAs, providing independent, vigorous enforcement of the data protection requirements set forth in the Privacy Shield framework. EU individuals will have access to multiple avenues to resolve concerns – at no cost to the individual – and will have an option to work with their local (national) DPA to resolve complaints. Additionally, the Privacy Shield framework includes certain safeguards and transparency obligations relative to U.S. governmental access to personal data. For the first time, U.S. government has provided the EU with written commitments including an assurance from the Office of the Director of National Intelligence that access of public authorities to personal data for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms.

The Privacy Shield framework includes significant advancements to improve transparency regarding personal data use, strengthen the protections provided by participants, and inform EU individuals more comprehensively about their rights under the program. But it is not without its critics. There are concerns about unfettered access to consumer data by intelligence and law enforcement officials. And the fact that the program is subject to annual reviews has led to questions over whether the law could change on a regular basis, or as happened last autumn, get struck down altogether.

To join the Privacy Shield, a U.S.-based company will be required to register and self-certify to the U.S. Department of Commerce and publicly commit to comply with the requirements of the new framework. These requirements for such participating companies ("participants") include and are not limited to:

- NOTICE:
  participants must review, update and publicize their privacy policies online and declare their commitment to comply with Privacy Shield and the specific notice requirements of the new framework

- DISPUTE RESOLUTION:
  EU individuals whose data is being processed by participants may lodge a complaint directly with a participant, which must respond to the complaint within 45 days; participants must provide, without cost to the EU individuals, independent recourse mechanisms to investigate and expeditiously respond to such complaints; participants must commit to binding arbitration at the EU individual's request to address complaints that have not otherwise been resolved through the processes set forth in the framework; and the participant may choose an EU DPA as its independent recourse mechanism provided that submission to DPA oversight is mandatory when a company handles employee data[2];

- COOPERATION WITH DEPARTMENT OF COMMERCE:
  participants must cooperate and respond promptly with the U.S. Department of Commerce to resolve complaints submitted by EU individuals (which can also be submitted by such individuals to their local data protection authorities, or "DPAs")

- PURPOSE LIMITATION:
  similar to the Safe Harbour framework, participants must limit personal information to that which is relevant for processing and pertains to the original purpose for which it was collected (absent subsequent consent by the individual)

- ONWARD TRANSFERS:
  participants must enter into contracts with third-party controllers and processors, regardless of location, to ensure adherence to the Privacy Shield framework and principles including the consent provided by the EU individual relative to the processing of his or her personal data

- ACCESS:
  EU individuals have a right to know if participants are processing their personal data and modify, correct or delete it under certain circumstances (such as data being inaccurate or being processed in violation of the requirements of Privacy Shield)

Once a U.S.-based company commits to the Privacy Shield framework, the commitment will be enforceable under U.S. law and will remain enforceable regarding any personal data processed during the self-certification period, even if a company is no longer a participating company.

Best Practice Guidelines

Although the EU Commission's adequacy decision represents a milestone achievement towards a more unified system of laws and regulations around the processing and protection of personal data between the EU and the U.S., detractors and skeptics remain vocal about the shortcomings of the new framework. Privacy Shield will likely be challenged by activists and ruled upon by European Courts (including the ECJ). Other EU-U.S. data protection and compliance-related issues to be addressed will also focus on the impacts to Privacy Shield and compliance in general resulting from "Bre-

xit" and the upcoming implementation of the EU General Data Protection Regulation in May 2018. Companies processing personal data of EU citizens need to be undertaking privacy impact assessments to analyze what personally identifiable information is collected, used, processed and shared, understand and appropriately remediate compliance gaps, and make intelligent risk-related decisions with the next three-year horizon in mind. Organisations conducting data transfers involving personal data from the EU are tasked with identifying and implementing a robust plan with built-in contingencies if the horizon should suddenly change. In addition, the Article 29 Working Party has confirmed that model contracts or binding corporate rules can still be used for transfers of personal data from the EU to the U.S. Companies involved in the transfer of personal data from the EU to the U.S., or companies transferring employee data, should review their policies and procedures in light of these new developments especially regarding the new General Data Protection Regulation, as it will impact not only companies that operate in the EU, but that do business with EU consumers or employ EU citizens.

1 See European Commission, "Guide to the EU-U.S. Privacy Shield" (http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf), 2016, p. 7.

2 Id. at 15.

Victorine Kossi

Der Weg zum EU-US Privacy Shield

Im Rahmen einer Klage des österreichischen Datenschutzaktivisten Max Schrems gegen die irische Datenschutzaufsicht wegen Facebooks Datenübertragungen in die USA erklärte der europäische Gerichtshof (EuGH) mit einem Urteil vom 6. Oktober 2015[1] das Safe-Harbor-Abkommen zwischen den USA und der europäischen Kommission für ungültig.

Um eine Datenübermittlung in die USA zu ermöglichen wurde im Jahr 2000 das sog. Safe-Harbor-Abkommen eingeführt, weil die USA als unsicheres Drittland nach EU-Datenschutzvorgaben gelten. Werden Daten in ein Drittland übermittelt, so müssen die Datenexporteure sicherstellen, dass dort ein angemessenes Datenschutzniveau herrscht.

Mit der Angemessenheitsentscheidung der Kommission vom 26. Juli 2000 konnten Unternehmen in den USA durch Selbstzertifizierung nach den Safe-Harbor-Grundsätzen Daten aus der EU rechtmäßig importieren. Dieses Abkommen diente Jahrzehnte lang EU/EWR ansässigen Unternehmen als Grundlage für den Datenexport in die USA. Mehr als 4000 Unternehmen nutzten diese Vereinbarung um personenbezogene Daten legal in die USA zu übermitteln.

Das Abkommen war aber höchst umstritten. Bemängelt wurden vor allem die massive Datenüberwachung durch amerikanischen Sicherheitsbehörden und die fehlenden Mechanismen zur Durchsetzung der Betroffenenrechte. Die Artikel-29-Arbeitsgruppe hatte bereits im Dezember 2014 auf diese Schwächen hingewiesen.

Seitdem das Abkommen vom EuGH aufgehoben wurde, bot Safe Harbor nun keinen sicheren Hafen mehr für den Export europäischer Daten. Es musste eine neue Lösung her.

Amerikanische und europäische Behörden führten intensive Gespräche, um eine Nachfolgevereinbarung für das Safe-Harbor-Abkommen auszuhandeln und abzuschließen. Am 2. Februar 2016 wurde eine erste politische Einigung erzielt. Das sogenannte EU-US Privacy Shield-Abkommen sollte einen neuen Rahmen für die Übermittlung personenbezogener Daten zwischen der EU und den Vereinigten Staaten unter Berücksichtigung der Anforderungen der EuGH-Entscheidung vorgeben

Die Kommission stellte am 29. Februar 2016 ein erstes Ergebnis vor. Die „Artikel-29-Arbeitsgruppe" lieferte dann am 13. April 2016 eine erste kritische Stellungnahme zu diesem Entwurf und riet zu Nachbesserung.

Eine neue Version des EU-US Privacy Shield wurde am 26. Mai 2016 per Entschließung durch das Europäische Parlament angenommen. Die Kommission konnte damit das Verfahren zur Annahme des neuen Abkommens am 12. Juli 2016 durch den Erlass einer Angemessenheitsentscheidung abschließen. Mit dieser Entscheidung soll das „EU - US-Schutzschild" ein hohes Schutzniveau für den Datentransfer bieten, das im Wesentlich mit den europäischen Anforderungen „gleichwertig" sei.

(Anfangs-)Vorbehalte durch die Artikel-29-Arbeitsgruppe und den europäischen Datenschutzbeauftragten

Bei der Ankündigung des neuen Abkommens im Februar 2016 bezeichnete die EU-Kommission dieses als „starken Rahmen", der das Vertrauen in die transatlantischen Datenströme zwischen der EU und den USA wieder herstellen soll.

Trotz verbreitetem Optimismus mahnte die Artikel-29-Arbeitsgruppe zur Vorsicht.

In ihrer Stellungnahme vom 13. April 2016[3] hegte die Artikel-29-Arbeitsgruppe Zweifel hinsichtlich der Konformität des neuen Abkommens mit den europäischen Datenschutzgrundsätzen. Ferner kritisierte sie mangelnde Klarheit der Bestimmungen des Abkommens und fehlende Präzisierung der Grundprinzipien des Datenschutzes, so wie sie im europäischen Datenschutzgesetz verankert sind.

Ihrer Ansicht nach tragen die Mechanismen zur Durchsetzung von Betroffenenrechten aufgrund ihrer Komplexität zu keinem wirksamen Schutz bei. Die Kritik der Artikel-29-Arbeitsgruppe wurde zum größten Teil vom Europäischen Datenschutzbeauftragten in seiner Stellungnahme vom 30. Mai 2016 aufgenommen. Der Europäische Datenschutzbeauftragte erklärte, das Abkommen sei nicht robust und würde einer erneuten rechtlichen Prüfung durch den europäischen Gerichtshof nicht standhalten. Ferner bräuchte eine Angemessenheitsentscheidung erhebliche Verbesserung im Hinblick auf die wichtigsten Grundsätze des Datenschutzes, mit besonderem Augenmerk auf die Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und den Anspruch auf Rechtsschutz.

Was ist neu durch den EU-US Privacy Shield?

Nach Ansicht der europäischen Kommission enthält das neue Abkommen eine Reihe wichtiger Verbesserungen im Vergleich zu dem vorherigen Safe-Harbor-Abkommen.

Die Europäische Kommission hat unter anderem von den amerikanischen Behörden zugesichert bekommen, Unternehmen, die personenbezogene Daten aus Europa importieren, stärker in die Pflicht zu nehmen und die Anwendung des Abkommens genauer zu überwachen. Die Federal Trade Commission (FTC) wird künftig Sanktionen verhängen können und gar teilnehmende Unternehmen wegen unlauterer und irreführender Geschäftspraktiken ausschließen können, wenn diese sich nicht an die Vorgaben des neuen Abkommens halten. Im Sinne der Transparenz müssen die zertifizierten Unternehmen ihre Datenschutzpolitik veröffentlichen.

Das Abkommen enthält auch zum ersten Mal schriftliche Verpflichtungen und Zusicherungen amerikanischer Behörden hinsichtlich des Zugriffs auf europäische personenbezogene Daten. Massenhafte und undifferenzierte Überwachung soll es nicht mehr geben. Vielmehr wurden genaue Bedingungen und Grenzen der Überwachung durch US-Behörden definiert.

Darüber hinaus verpflichten sich die Vereinigten Staaten alternative Verfahren und Mechanismen zur Beilegung von Streitigkeiten und Möglichkeiten, sich an einen Ombudsmann zu wenden, zu schaffen sowie Rechte betroffener Europäer besser zu schützen.

Zu diesen ausgehandelten Punkten wurden aber auch weitere Klarstellungen insbesondere zur Sammelerhebung von Daten, der Stärkung der Ombudsmannstelle und präzisere Verpflichtungen für Unternehmen in Bezug auf Beschränkungen für die Speicherung und die Weitergabe von Daten vereinbart.

Denn die EU-Kommission war seit der Vorlage des Entwurfs des Datenschutzschilds im Februar 2016 bemüht, den Stellungnahmen der Europäischen Datenschutzaufsichtsbehörden, des Europäischen Datenschutzbeauftragten sowie der Entschließung des Europäischen Parlaments Rechnung zu tragen. Das neue EU-US Privacy Shield beruht auf folgenden Grundsätzen:

- Strengere Auflagen für Unternehmen, die Daten verarbeiten
- Klare Schutzvorkehrungen und Transparenzpflichten beim Datenzugriff durch US-Behörden
- Wirksamer Schutz der Rechte des Einzelnen
- Gemeinsame jährliche Überprüfung

Einzelheiten des Abkommens können aus dem Fact Sheet EU-US Privacy Shield FAQs entnommen werden.[4]

Das Abkommen wurde den Mitgliedstaaten bereits mitgeteilt. Amerikanische Unternehmen, die das EU-US Privacy Shield nutzen wollen, können sich ab dem 1. August 2016 nach den neuen Regeln zertifizieren lassen. Das US-Handelsministerium (Federal Trade Commission) stellt der Öffentlichkeit auf seiner Webseite eine Liste der zertifizierten Unternehmen zur Verfügung.[6]

Ende gut, alles gut?

Es muss festgehalten werden, dass das Abkommen eine große Erleichterung für die etwa 4000 Unternehmen ist, die Safe Harbor genutzt haben. Mit diesem neuen Abkommen verlassen sie den Bereich der Rechtsunsicherheit, in dem sie seit der Absetzung des Safe-Harbor-Abkommens gefangen waren.

Die europäische Kommission stellte selbst in einer Mitteilung vom 29. Februar 2016[7] fest, dass die Übermittlung und der Austausch personenbezogener Daten ein wesentlicher Bestandteil der engen Beziehungen zwischen der Europäischen Union und den Vereinigten Staaten sowohl im Handelsbereich als auch im Bereich der Strafverfolgung sei.

Die Nachhaltigkeit dieser Lösung ist jedoch zweifelhaft, denn das Abkommen bleibt trotz aller Nachbesserungen umstritten.

Wie Safe Harbor bleibt der EU-US Privacy Shield ein sehr flexibler Mechanismus, der erst durch Selbstzertifizierung greift. Es ist nicht absehbar, ob die nach harten Verhandlungen abgerungenen Zugeständnisse eingehalten werden. Die grundsätzlichen Bedenken wegen der wenig transparenten Massenüberwachung durch die US-Geheimdienste dürften bestehen bleiben.

Es gab keine Zusicherung seitens der amerikanischen Behörden künftig keine Daten mehr von Unternehmen im großen Stil abzugreifen, sondern nur ihren Umfang zu reduzieren und soweit wie möglich ihre Verwendung auf sechs Ziele der nationalen Sicherheit (Spionage, Terrorismus, Massenvernichtungswaffen, Gefahren für die Cyber-Sicherheit, auf die Streitkräfte oder transnationale kriminelle Bedrohungen) zu begrenzen. Diese Liste wird jährlich überarbeitet. Inwieweit die Kommission diese Liste beeinflussen kann, bleibt ungewiss.

Das Abkommen sieht außerdem den Einsatz eines „Privacy Shield Ombudsmann“ als unabhängige Beschwerdestelle und Vermittler zwischen europäischen Bürgern und amerikanischen Geheimdiensten, die ihre Befugnisse

missbrauchen, vor. Aber genau die Unabhängigkeit dieses Ombudsmanns wird in Frage gestellt. Die Mechanismen zu Streitbeilegung bleiben für einzelne EU-Bürger sehr komplex und undurchsichtig.

Die Stellungnahme der Artikel-29-Arbeitsgruppe war nach der Verabschiedung des Abkommens mit großer Spannung erwartet worden. In ihrer am 26. Juli 2016 veröffentlichten Stellungnahme[8] begrüßte sie die Berücksichtigung ihrer Anforderungen, bemängelt jedoch weiterhin, dass bestimmte Aspekte, wie die Nutzung der Daten für kommerzielle Zwecke, Vorbehalte zur Nutzung der Daten durch Auftragnehmer, und der Zugriff der US-Behörden auf die Daten nicht geklärt bzw. nicht eindeutig genug geregelt wurden. Die Artikel-29-Arbeitsgruppe hat sich vorgenommen in einem Jahr die Wirksamkeit des Privacy Shields zu bewerten. Eine negativere Bewertung hätte wahrscheinlich die Robustheit des Abkommen stark geschwächt.

Es ist aber zu erwarten, dass Aufsichtsbehörden nationale Gerichte oder den EuGH anrufen und somit das neue Abkommen erneut auf die Probe stellen werden.

1 EuGH, Urteil vom 6.10.2015 - C-362/14, Maximillian Schrems / Data Protection Commissioner

2 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf

3 Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision

4 http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm

6 https://www.privacyshield.gov/list besucht am 10.09.2016

7 Communication from the Commission to the European Parliament and Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf

8 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

Frank Spaeing

Der EU-US Privacy Shield aus Sicht der DVD

Nun ist er also da, der EU-US Privacy Shield.

Wie in den zwei vorangegangenen Artikeln schon geschrieben wurde, hat die EU-Kommission am 12.07.2016 die Angemessenheitsentscheidung zu Gunsten des Regelwerks zum „Datenschutz-Schutzschild“ beschlossen.

Die Deutsche Vereinigung für Datenschutz hat seit dem wegweisenden Urteil des EuGH[1] vom 06.10.2015 in mehreren Pressemitteilungen den Weg dahin mahnend begleitet. Im Nachhinein betrachtet haben diese Mahnungen (wie realistisch zu erwarten war) nicht viel genutzt.

Schon am 13.10.2016[2] forderten wir, dass nach dem Urteil über einer der möglichen Rechtsgrundlagen für Europäische Unternehmen zur Übertragung personenbezogener Daten in die USA alle beteiligten Parteien zügig auf eine Nachfolgereglung hinarbeiten sollten, die alle Forderungen des Urteils umsetzen würde.

Die europäischen Aufsichtsbehörden hatten in ihrer Entscheidung vom 16.10.2015[3] eine dreimonatige Übergangsfrist eingeräumt, in der sie Unternehmen, die weiterhin auf Grund des Safe-Harbor-Abkommens Daten in die USA übertragen, nicht sanktionieren wollten, um Zeit für die Schaffung und dann Nutzung einer Nachfolgeregelung zu geben.

Anfang Februar 2016 gab es dann eine Pressekonferenz[4], bei der die zuständige EU-Kommissarin Věra Jourová im Beisein ihres amerikanischen Verhandlungspartners (der durchaus überrascht schien) das Ergebnis verkündete, dass die EU mit den USA ein Nachfolgeabkommen beschlossen habe, welches aber erst in den nächsten Wochen[5] der Öffentlichkeit im Detail gezeigt werden könne.

Auch dieses Ereignis begleiteten wir mit einer kritischen Pressemitteilung[6], in der wir u.a. feststellten, dass die wesentliche Arbeit beim Aushandeln des Nachfolgers von Safe Harbor noch nicht getan sei und diese Pressekonferenz nur dazu diene, die von den europäischen Aufsichtsbehörden festgelegte Stillhaltefrist zu verlängern.

Ende Februar war es dann soweit, es wurde von der EU-Kommission das EU-US Privacy Shield vorgestellt[7], wiederum begleitet durch eine DVD-Pressemitteilung[8], aus der ich mich hier gerne selbst zitiere:

„Es ist für uns nicht nachvollziehbar, wie die EU-Kommissare Ansip und Jourává die Behauptung aufstellen können, das Datenschutzschild entspräche den Anforderungen des EuGH in Sachen

Grundrechtsschutz und Rechtsschutzmöglichkeit. Aus den Dokumenten ergeben sich nicht im Ansatz effektive Begrenzungen der Massenüberwachung durch Sicherheitsbehörden wie die NSA und ebenso keine wirksamen Datenschutzinstrumente gegenüber US-Firmen.“

Ein großer Wurf sieht anders aus.

Auch die von der EU-Kommission zum EU-US Privacy Shield bereitgestellte FAQ[9] brachte keine wesentlichen neuen Erkenntnisse.

Die Artikel-29-Arbeitsgruppe kommentierte in ihrer Veröffentlichung[10] vom 13.04.2016:

„The Privacy Shield is the first adequacy decision that has been drafted since the texts of the GDPR were agreed in principle. Still, many of the improvements on the level of data protection offered to individuals are not reflected in the Privacy Shield. The WP29 therefore recommends that a review of this adequacy decision, as well as of the adequacy decisions issued for other third countries, should take place shortly after the GDPR enters into application.“

Eine wohlwollende Würdigung sieht anders aus.

Am 01.07.2016 hat die Artikel-29-Arbeitsgruppe in einer Pressemitteilung[11] ihre Forderungen noch einmal bestätigt. Auch wir haben am gleichen Tag eine Presseerklärung[12] herausgegeben, in der wir klarstellten, dass die zentralen Forderungen des EuGH-Urteils vom 06.10.2015 unserer Meinung nach im EU-US Privacy Shield nicht erfüllt seien und dass Zugeständnisse an die USA im Nachklang des BREXIT auch auf die anstehenden Verhandlungen mit UK Auswirkungen haben würden.

Unbeeinflusst davon hat am 12.07.2016 die EU-Kommission die Angemessenheitsentscheidung zum EU-US Privacy Shield beschlossen. Laut der Pressemitteilung hatte die Kommission auf dem Weg zu dieser Entscheidung mit allen, auch den europäischen Aufsichtsbehörden, zusammengearbeitet:

„We have worked together with the European data protection authorities, the European Parliament, the Member States and our U.S. counterparts to put in place an arrangement with the highest standards to protect Europeans‘ personal data.“

Ob die europäischen Aufsichtsbehörden sich dieser Tatsache bewusst waren?

In unserer Presseerklärung[13] vom 12.07.2016 stellten wir die Langlebigkeit dieser Entscheidung in Frage und fragten uns, ob der EuGH bei gleichbleibender Rechtsprechung lange brauchen werde um dem EU-US Privacy Shield ebenso wie Safe Harbor die Rechtmäßigkeit abzusprechen.

Am 26.07.2016 äußerte sich die Artikel-29-Arbeitsgruppe mit einer Presseerklärung[14], in der sie grundsätzlich die Verbesserungen des EU-US Privacy Shield gegenüber Safe Harbor lobte. Aber dann auch sofort wieder auf die Defizite hinwies und klarstellte, dass das erste jährliche Review (die jährlichen Überprüfungen sind eine der faktisch vorhandenen Verbesserungen zu Safe Harbor) zum Schlüsselmoment beim Beurteilen der Robustheit und Effizienz des EU-US Privacy Shield werde.

Sie fordern eine uneingeschränkte Beteiligung bei diesem Review und stellen weitergehende Konsequenzen aus diesem Review für die anderen momentan existierenden rechtlichen Möglichkeiten (Binding Corporate Rules und EU-Standard-Vertragsklauseln) zur Übertragung von personenbezogenen Daten in die USA (und in Drittstaaten generell) in Aussicht:

„The first joint annual review will therefore be a key moment for the robustness and efficiency of the Privacy Shield mechanism to be further assessed. In this regard, the competence of DPAs in the course of the joint review should be clearly defined. In particular, all members of the joint review team shall have the possibility to directly access all the information necessary for the performance of their review, including elements allowing a proper evaluation of the necessity and proportionality of the collection and access to data transferred by public authorities. When participating in the review, the national representatives of the WP29 will not only assess if the remaining issues have been solved but also if the safeguards provided under the EU-U.S. Privacy Shield are workable and effective. The results of the first joint review regarding access by U.S. public authorities to data transferred under the Privacy Shield may also impact transfer tools such as Binding Corporate Rules and Standard Contractual Clauses.“

In der Zwischenzeit werden sich die europäischen Aufsichtsbehörden auf die proaktive Unterstützung der europäischen Bürger bei der Wahrung ihrer Rechte aus dem EU-US Privacy Shield und auf die Bereitstellung weiterführender Informationen zum EU-US Privacy Shield und die damit verbundenen Arbeitsweisen beschränken:

„In the meantime, and now that the Privacy Shield has been adopted, with the Schrems judgment and opinion WP238 in mind, the DPAs within the WP29 commit themselves to proactively and independently assist the data subjects with exercising their rights under the Privacy Shield mechanism, in particular when dealing with complaints. The WP29 will soon provide information to data controllers about their obligations under the Shield, comments on the citizens’ guide, suggestions for the composition of the EU centralized body and for the practical organisation of the joint review.“

Auch dies hört sich nicht wie eine überschäumende Laudatio an. Was ja auch nicht zu erwarten war. Tatsächlich hatten sich die Bürgerrechtsbewegungen, die gegen den EU-US Privacy Shield angetreten waren, deutlich mehr erhofft[15] (wie unter anderem aus unseren im Artikel erwähnten Presseerklärungen klar hervorgeht).

Dass die deutschen Aufsichtsbehörden sich überaus laut zurückgehalten haben lässt vermuten, dass sie sich bereits auf die enge Zusammenarbeit im Rahmen des Datenschutzausschusses gemäß der EU-DSGVO vorbereiten. In persönlichen Gesprächen waren die Meinungsäußerungen von Mitarbeitern einiger deutscher Aufsichtsbehörden zum EU-US Privacy Shield tatsächlich deutlich weniger wohlwollend.

Mittlerweile hatte ja auch Anfang Juni 2016 die hamburgische Aufsichtsbehörde die ersten Bußgelder[16] gegen Unternehmen verhängt, die nach dem EuGH-Urteil noch auf Safe Harbor gesetzt hatten. Über die Höhe der Bußgelder kann sicherlich diskutiert werden, in der Presseerklärung wird jedoch deutlich, dass diese deutlich geringer seien als es die nächsten sein werden, falls weiterhin Unternehmen dabei erwischt würden, dass

sie sich nicht um eine funktionierende Rechtsgrundlage gekümmert hätten.

Seit dem 01.08.2016 ist der EU-US Privacy Shield nun voll funktionsfähig[17] und US-Unternehmen können sich auf den Seiten des US Handelsministeriums (FTC) in der Liste der selbst verpflichteten Unternehmen führen lassen, wenn sie sich an die Regeln des EU-US Privacy Shield halten[18].

Perfiderweise haben sie neun Monate Zeit, bevor sie auch all diese Regeln einhalten müssen, auf die sie sich selbst verpflichtet haben[19]. Was verwundert, da die Anforderungen nicht wesentlich von denen gemäß Safe Harbor abzuweichen scheinen.

Trotzdem gilt der EU-US Privacy Shield nach Aussagen der EU-Kommission bereits ab dem 01.08.2016 als Rechtsgrundlage!

Im Vergleich zum Aufwand, den deutsche Unternehmen betreiben müssen, um eine wirksame Auftragsdatenverarbeitung gemäß § 11 BDSG zu vereinbaren[20], wirkt dieses Regelwerk geradezu lächerlich schwach[21].

Die EU-Kommission hat außerdem einen Ratgeber für Beschwerden gegen Unternehmen, welche die Datenschutzstandards des EU-US Privacy Shield nicht einhalten, veröffentlicht[22]. Dieser Leitfaden[23] enthält neben den Rechten der Bürger und Pflichten der US-Unternehmen, die sich nach dem EU-US Privacy Shield verpflichtet haben, eine Zusammenstellung der Möglichkeiten für den Fall, dass ein US-Unternehmen seinen Verpflichtungen nicht nachkommt.

Den Betroffenen steht ein kostenloses Verfahren zur alternativen Streitbeilegung (genannt Alternative Dispute Resolution) zur Verfügung. Zusätzlich ist es ihnen jederzeit möglich, sich an die nationalen Datenschutzbehörden in ihrem EU-Mitgliedstaat zu wenden, welche dann gemeinsam mit der FTC der Beschwerde nachgehen. Als letztes Mittel steht den Betroffenen außerdem ein Schiedsverfahren offen.

Für den Fall, dass es um Rechtsschutzbegehren geht, die den Bereich der nationalen Sicherheit betreffen, wurde zusätzlich eine „von den US-Geheimdiensten unabhängige Ombudsstelle“ eingerichtet.

Hier werden die europäischen Aufsichtsbehörden also gut zu tun haben, um die europäischen Bürger proaktiv bei der Durchsetzung ihrer Rechte zu unterstützen, da die Mechanismen zur Streitbeilegung für einzelne EU-Bürger komplex und undurchsichtig bleiben. Einfach ist anders.

Nun ist er also da, der EU-US Privacy Shield. Wir sind gespannt, wie lange er bleibt…

1 Siehe http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=frst&part=1&cid=115283

2 Siehe https://www.datenschutzverein.de/wp-content/uploads/2015/10/2015-10-12_DVD-PM_EuGH_zu_Safe_Harbor.pdf

3 Siehe http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

4 Siehe http://europa.eu/rapid/press-release_SPEECH-16-221_en.htm

5 Siehe http://europa.eu/rapid/press-release_IP-16-216_en.htm

6 Siehe https://www.datenschutzverein.de/wp-content/uploads/2016/02/2016-02-03-DVD_zu_EU-US-Privacy_shield.pdf

7 Siehe http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm

8 Siehe https://www.datenschutzverein.de/wp-content/uploads/2016/03/2016-03-01-DVD_schockiert_ueber_EU-US-Privacy_shield.pdf

9 Siehe http://europa.eu/rapid/press-release_MEMO-16-434_en.htm

10 Siehe http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

11 Siehe http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160701_wp29_press_release_eu_us_privacy_shield_en.pdf

12 Siehe https://www.datenschutzverein.de/wp-content/uploads/2016/07/2016-07-01-DVD-PE-EU-US-PrivacyShield.pdf

13 Siehe https://www.datenschutzverein.de/wp-content/uploads/2016/07/2016-07-12-DVD-PE-EU-Kommssion_beschliesst_PrivacyShield.pdf

14 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

15 Siehe u.a. https://edri.org/transatlantic-coalition-of-civil-society-groups-privacy-shield-is-not-enough-renogitation-is-needed/

16 Siehe https://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-datenuebermittlungen-in-die-usa.html?tx_ttnews%5BbackPid%5D=170&cHash=d21026cc72d2a53525c7c40d6cbaa6e2

17 Siehe http://ec.europa.eu/justice/newsroom/data-protection/news/160801_en.htm

18 Siehe hierzu die Artkel von Frau Dr. Kossi und Frau Rothmann in dieser DANA

19 Dieses galt für alle Unternehmen, die sich in den ersten beiden Monaten selbst auf den EU-US Privacy Shield verpflichtet haben.

20 U.a. § 11 Absatz 2, Satz 4 BDSG: „Der Aufraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Aufragnehmer getrofenen technischen und organisatorischen Maßnahmen zu überzeugen.“

21 Beim EU-US Privacy Shield warten wir erst einmal neun Monate auf die Zusicherung der Compliance? Und europäische Unternehmen übermitteln trotzdem sofort die Daten? Und das ist rechtskonform und entspricht den Anforderungen des EuGH-Urteils?

22 Im Moment steht das Dokument nur auf Englisch zur Verfügung, siehe http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf

23 Kurz vor der Drucklegung gab es dann (zumindest) eine deutsche Übersetzung: http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf

Frank Spaeing

Pokémon GO und Datenschutz?

Pokémon GO ist ein weltweites Phänomen. In den letzten Wochen hat sicherlich jeder schon Gruppen von Smartphone-Nutzern gesehen, die sich in Parks, an Kreuzungen, bei Kirchen, quasi überall versammelt haben, auf ihre Smartphones starren und ab und zu auf diesen hektische Bewegungen ausführen. Diejenigen, die Pokémon GO noch nicht kennen, fragen sich nun, was sie da eigentlich beobachten.

Pokémon GO ist eines der neuen Augmented Reality (AR) Spiele, sprich im Smartphone wird das von der Kamera aufgenommene Bild mit virtuellen Elementen, die das Smartphone hinzufügt, angereichert (augmented). Schon vorher gab es solche Spiele, Ingress[1] ist ein vielleicht bekanntes Beispiel, bei dem seit Ende 2013 Spieler (auch in Deutschland) in zwei konkurrierenden Gruppen versuchen, möglichst große öffentliche Bereiche unter ihre virtuelle Kontrolle zu bringen.

Pokémon GO funktioniert anders. Hier geht es darum, dass die Spieler virtuelle Pokémon fangen, diese trainieren, entwickeln und in virtuelle Kämpfe gegen andere Pokémon schicken.

Was macht dieses Spiel nun so faszinierend[2]? Zum einen trifft es scheinbar genau den Nerv derjenigen, die in ihrer Jugend Pokémon Spiele auf Nintendo-Konsolen gespielt haben. Zum andern verbindet es auf gekonnte Art Spielen und Bewegung bis hin zu Interaktion mit anderen Spielern im echten Leben. Es gibt diverse skurrile Geschichten rund um Pokémon GO:

Ein Massennachtwandern mit ca. 1000 Teilnehmern durch Hannover[3]; Diebe, die ihre Opfer durch Pokémon GO gefunden haben; Bundeswehrmanöver mit scharfen Waffen, die wegen über den Truppenübungsplatz laufender Pokémon GO Spieler abgebrochen werden mussten[4]; Beinahe- und echte Verkehrsunfälle, da Spieler während der Fahrt Pokémons gejagt haben[5]; Pokémon GO Spieler, die den Verkehr lahm legen[6]; Pokémon GO Spieler, die über Bahngleise geirrt sind[7]; (u.a. Holocaust-) Gedenkstätten, die nicht als Spielstätten (sogenannte Pokéstops) missbraucht werden wollen[8]; Krankenhäuser, die Pokémons unwissentlich beherbergen und sich über die Menschenmengen wundern, die plötzlich durch die Stationen pilgern[9]; Straßenbahnen, die nur für Pokémon GO Spieler fahren[10]; Privatleute, die sich über Nächtens durch ihre Vorgärten irrende Pokémon GO Spieler wundern[11]; Taxi-Unternehmen, die Pokémon GO Fahrten zum Flatrate-Tarif anbieten[12]; Unternehmen, die unbedingt ihre Ladengeschäfte als Pokéstops ins Spiel integriert haben wollen[13]; kluge Menschen, die anderer Leute Smartphones gegen Geld spazieren führen, damit diese derweil neue Pokémons ausbrüten[14]; Länder, die die Nutzung von Pokémon GO verbieten[15]; Pokémon GO Spieler, die sich bei der Jagd nach Pokémon in Lebensgefahr bringen[16]; Musiker, die sich entweder bei ihren Konzerten beschweren, dass das Publikums, während sie spielen, gefälligst zuschauen und keine Pokémons jagen sollen, oder die sich lachend ins Bild neben das Pokémon stellen[17]; selbst die KfW-Bank wirbt bei Twitter damit, dass zwei ihrer Filialen Pokéstops sind[18]…

Und das obwohl das Spiel offiziell erst seit dem 13.07.2016 in Deutschland verfügbar ist. Der weltweite Start des Spieles war am 06.07.2016 in den USA, Australien und Neuseeland. Und innerhalb weniger Tage hat dieses Spiel alle Veröffentlichungsrekorde gebrochen[19], ist im Juli 2016 in Googles wie auch in Apples App-Store die unangefochtene Nr. 1 bei den Downloads gewesen. Pokemon Go ist mittlerweile nach einer Studie in den USA auf 5% aller Android-Smartphones installiert[20], Tinder, eine beliebte Dating-Plattform, nur auf 2%[21]. Der Börsenwert von Nintendo ist zwischenzeitlich fast aufs Doppelte gestiegen (und auch schon wieder eingebrochen)[22], obwohl Nintendo gar nicht der Hersteller des Spieles ist. Das ist Niantic, ein Google-Spin-Off, welches auch schon Ingress auf den Markt gebracht hat.

Und obwohl die Anzahl der täglichen Nutzer im August um ein Viertel zurück gegangen ist, sind es immer noch mehr als 30 Millionen Personen, die täglich Pokémon GO nutzen[23].

Was hat Pokémon GO nun mit Datenschutz zu tun?

Leider Einiges: Zum einen ist das Thema Selbstdatenschutz zu nennen, zum anderen ist die Datensicherheit ein großes Problem bei dem Spiel, Spieler sollten aktiv über Selbstschutz nachdenken und auch für Unternehmen kann das Spiel Probleme bereiten.

Doch der Reihe nach.

Selbstdatenschutz:

Eingeräumte Rechte und Zugriff auf personenbezogene Daten

Pokémon GO benötigt, um gespielt werden zu können, natürlich Rechte auf dem Smartphone. Es benötigt den Zugriff auf die Kamera, um an den entsprechenden Stellen Pokémons in das reale Bild einzublenden, es benötigt die Standortdaten, um die Spieler zu den Pokémons zu lotsen. Neben diesen offensichtlich notwendigen Daten werden noch weitere Daten erfasst, wie u.a. die lückenlose Erfassung aller Aktionen im Spiel und aus den Standortdaten generierte Bewegungsprofile.

Mit den Nutzungsbedingungen räumt Niantic sich selbst und dritten umfassende Nutzungsrechte an den Daten ein. Schon jetzt ist es Realität, dass nur wenige Nutzer konsequent Nutzungsbedingungen und AGBs und Datenschutz-

hinweise lesen, deswegen werden auch bei Pokémon GO die Wenigsten wissen, was sie genau akzeptieren.

Es ist auf jeden Fall nicht möglich, das Spiel anonym zu spielen.

Die Pokémon Company speichert von Pokémon-Spielern personenbezogene Daten wie den Namen, Mail-Adresse, Telefonnummer und nimmt sich in seinen Geschäftsbedingungen heraus, diese auch mit demographischen Informationen wie Alter, Geschlecht, Geburtsdatum, Hobbys und Präferenzen in Bezug auf Spielzeuge und Spiele zu verknüpfen und an Dritte weiterzugeben.

Eine interessante Anekdote ist es an dieser Stelle sicherlich, dass der Chef von Niantic vorher für Google Street Maps zuständig war, die bei ihren Straßenerfassungsfahrten ja auch diverse andere Daten (bis hin zu WLANs) erfasst hatten[24].

Außerdem benötigt das Spiel einen Account. Als das Spiel veröffentlicht wurde, war dafür im Wesentlichen nur den Google-Account nutzbar, mittlerweile geht es auch mit einem Account beim Pokémon Trainer Club[25]. Das Problem der Verknüpfung mit dem Google Account war, dass sich Niantic hier umfassende Nutzungsrechte (unter anderem auch des E-Mail-Accounts) einräumte. Seit der Version 1.02 haben sich die eingeräumten Nutzungsrechte reduziert.

Hier ist es auf jeden Fall sinnvoll, falls jemand jetzt erst mit dem Spiel beginnen will, einen neuen Account (sei es bei Google oder beim Pokémon Trainer Club) anzulegen und diesen für das Spiel zu nutzen um den Zugriff auf personenbezogene Daten in den Haupt-Accounts zu verhindern. Allerdings ist es nur unter Verlust aller bisher erspielten Daten und Spielstände möglich, von einem Account auf einen anderen zu wechseln.

Neben den oben genannten vielfältigen Datenerhebungen fehlen an vielen Stellen nach deutschem Datenschutzrecht konkrete Einwilligungen in Übertragungen (zum Beispiel an die oben genannten Dritten). Speziell erwähnt sei hier noch eine sehr versteckte und nach deutschem Recht so wohl nicht zulässige Klausel, die besagt, dass die Spieler, wenn sie nicht konkret innerhalb von dreißig Tagen widersprechen, mit Akzeptieren der Nutzungsbedingungen auf jegliche Klagerechte vor Schiedsgerichten verzichten („Wenn Sie Niantic keine Schiedsverfahrens-Verzichtserklärung innerhalb der 30-Tagesfrist zukommen lassen, wird davon ausgegangen, dass Sie wissentlich und vorsätzlich von Ihrem Recht, jede Unstimmigkeit vor Gericht klären zu lassen, zurückgetreten sind [...]“).[26]

Zu guter Letzt ist das Thema Löschen von personenbezogenen Daten und die Weitergabe an Regierungen und Strafverfolgungsbehörden unbefriedigend und meist intransparent für die Spieler geregelt.

Auch der Verbraucherzentrale Bundesverband (vzbv) hat übrigens Niantic schon wegen der Nutzungsbedingungen abgemahnt[27].

In-App-Käufe

Pokémon GO ist ein sogenanntes Freemium-Spiel. Man kann es kostenlos herunterladen, installieren und spielen. Aber an vielen Stellen wird durch das Spiel gesteuert recht bald das Bedürfnis geweckt, dass das doch auch schneller gehen muss. Diese Abkürzungen kann man sich über Pokémünzen erkaufen. Diese gibt es für reale Geldbeträge (von 0,99 € für 100 Pokémünzen bis hoch zu 99,99 € für 14.500 Pokémünzen) zu kaufen.

Da ein recht großer Teil des Zielpublikums sicherlich noch nicht volljährig ist, sollten hier die Eltern besonders aufpassen, dass sich nicht schnell große Summen addieren. Auch Erwachsene sollten im Zweifelsfall gut abwägen, ob es sich lohnt, für ein Spiel (im Zweifelsfall viel) Geld auszugeben.

Datensicherheit

Probleme mit verseuchten, nicht-offiziellen Apps

Pokémon GO wurde, obwohl es erst am 13.07.2016 offiziell in Deutschland (und auch in anderen Ländern) veröffentlicht wurde, trotzdem schon gespielt. Die Spieler konnten sich über mehr oder weniger offizielle und sicherlich meist weniger sichere Wege die Spieleinstallationsdateien (APKs) herunterladen und die Spiele installieren. Allerdings gab es genügend Installationspakete, die Trojaner- oder Virenverseucht waren. Deswegen galt zu Beginn und gilt auch weiterhin: Pokémon GO im Eigeninteresse nur über die offiziellen App-Stores laden und installieren.

Mittlerweile ist es so, dass es hunderte Trittbrettfahrer-Apps in (zumindest) den Google-App-Stores gibt[28], die außer dem Namen wenig mit dem Spiel gemein haben und versuchen, Nutzern unberechtigt Daten abzuziehen. Hier gilt es sehr sorgfältig zu prüfen, ob eine App wirklich zusätzlich zum Hauptspiel nötig ist, um Pokémon GO spielen zu können[29].

Auch gibt es mittlerweile für Windows eine PC-App für Pokémon GO, diese enthält allerdings im Wesentlichen nur einen Verschlüsselungs-Trojaner[30].

Akkulaufzeit

Eine Problematik, die mit Datensicherheit nicht viel zu tun hat, aber vielleicht trotzdem die Verfügbarkeit und auch Nutzbarkeit des Smartphones an sich beeinträchtigen kann, ist die schnell sinkende Akkulaufzeit. Das Spiel benötigt reichlich Akkuleistung, da sowohl der Grafikchip als auch die Kamera und natürlich auch das Display im Betrieb im Freien am Akku nagen. Es sind schon viele Spieler mit Rucksäcken gesichtet worden, in denen neben der Verpflegung (Bewegung an der frischen Luft macht Appetit, dazu unten mehr) auch zusätzliche Akkupacks transportiert werden[31].

Selbstschutz

Wie schon bei den oben genannten skurrilen Geschichten erwähnt, hat es bereits Pokémon GO Spieler gegeben, die unaufmerksam am Straßenverkehr teilgenommen haben (als Autofahrer oder als Fußgänger bzw. Radfahrer) und so entweder in Unfälle verwickelt wurden oder nur knapp diesen entgangen sind.

Hierzu müssen die Spieler berücksichtigen, dass die Nutzung von Smartphones im Straßenverkehr (als Autofahrer) zum einen Geldbuße und einen Punkt in Flensburg bedeutet, dass zum anderen im Falle eines Unfalles die Versicherungen bei der nachgewiesenen Nutzung des Smartphones von grober Fahrlässigkeit ausgehen und somit den Kaskoschutz versagen können[32].

Auch unbedarft durch die Gegend zu laufen, immer mit Blick aufs Smartphone-Display, kann gefährlich sein, wie mehrere Beinahe-Unfälle auf Bahnschienen und der Vorfall auf dem deutschen Truppenübungsplatz gezeigt haben. Hier sollten die Spieler tatsächlich vorher nachdenken und ab und zu mal den Realitäts-Check durchführen („Wo bin ich gerade und was mache ich gerade im echten Leben?“).

Auch sollte nicht jede Gegend gerade zu nächtlicher Zeit alleine aufgesucht werden, da es zumindest in den USA schon Verbrecher gegeben hat, die sich im Spiel besonders beliebte und für ihre Zwecke praktische Gegenden ausgesucht und dort Pokémon GO Spieler beraubt haben[33].

Wie sind Unternehmen von Pokémon GO betroffen?

Grundsätzlich sind natürlich die meisten Probleme, die bisher genannt wurden (zum Beispiel In-App-Käufe und Akkulaufzeiten) auch für Unternehmen relevant, wenn diese die Nutzung von dienstlichen Smartphones im privaten Kontext zulassen, denn dann sind es ja Dienstsmartphones, auf denen diese Probleme auftreten können.

Auch die Datenschutzfragen betreffen dann auf einmal das Unternehmen, denn die sich auf dem Smartphone befindlichen Daten sind ja dann auch dienstlicher Natur und hierbei hat das Unternehmen als verantwortliche Stelle sicherzustellen, dass personenbezogene Daten nicht unerlaubt Dritten zur Kenntnis gelangen und außerdem hat ja auch jedes Unternehmen Interesse daran, Geschäftsgeheimnisse angemessen zu schützen.

Zusätzlich kann, dadurch, dass die Spieler ja mit aktiven Kameras, die durch eine Fremdsoftware gesteuert werden, über Firmengelände laufen, auch das Thema Werksspionage relevant werden. Zum einen, weil kaum jemand weiß, was genau mit den Daten bei Niantic und den sonstigen berechtigen Dritten passiert, zum anderen, weil sicherheitsbewusste Unternehmen ähnlich wie die Bundeswehr bei ihrem Manövervorfall natürlich auch zu dem Schluss kommen können, dass sich (Wirtschafts-)Spione unter dem Deckmantel des Pokémon GO Spielens „zufällig“ in sensible Bereiche verirren können.

Hier kann ein Unternehmen u.a. über entsprechende Regelungen zur Nutzung von dienstlichen und auch privaten Smartphones gegensteuern[34].

Sollte das Unternehmen mit seinen Betriebsstätten als Pokéstop im Spiel installiert sein und nicht wie die KfW-Bank dieses auch noch als Vorteil empfinden, bleibt nur der Weg sich an den Anbieter Niantic mit einer entsprechenden Beschwerde zu wenden[35] und bis zur Löschung aus dem Spiel die Sicherheitsmaßnahmen der Zugangs- bzw. Zutrittskontrolle entsprechend zu erhöhen.

Gibt es auch Positives?

Neben den genannten Problematiken und neuen Themen, mit denen sich Spieler und Unternehmen befassen müssen, soll aber auch über die positiven Aspekte des Spieles gesprochen werden:

Es gibt bereits mehrere Ärzte, die sich positiv über Pokémon GO geäußert haben, da es die Spieler (vorsichtiges Verhalten sei jetzt einmal vorausgesetzt) ins Freie treibt und das gerade für eher bewegungsfaule Menschen durchaus förderlich ist.

Und mal abgesehen davon, dass es mitunter schon komisch wirkt, wenn Gruppen von Menschen auf ihre Smartphones starrend in der Gegend stehen oder sich langsam in ihr bewegen, gibt es auch schon reichlich Pokémon GO Spieler, die die unerwartete Interaktion mit Mitspielern und die sich daraus ergebenden neuen Kontakte durchaus schätzen[36].

Ein Fazit

Wenn Sie also das Spielvergnügen dem Selbstdatenschutz vorziehen, im Rahmen dessen, was in dem Spiel möglich ist, bestmöglich auf sich selbst und Ihre Sicherheit achten und wenn Sie die geltenden Regelungen in Ihren Unternehmen beachten, dann kann die Nutzung von Pokémon GO, mal abgesehen vom sicherlich vorhandenen Spielspaß, auch durchaus den einen oder anderen zusätzlichen Bonus bereithalten.

Oder doch nicht? Lesen Sie vielleicht doch erst den folgenden Artikel von Roland Appel.

Bis dahin können Sie ja in der unangereicherten Natur spielen[37].

1 Siehe https://de.wikipedia.org/wiki/Ingress_(Spiel)

2 Siehe http://www.heise.de/tr/blog/artikel/Dark-side-of-Pokemon-3272397.html

3 Siehe http://www.heise.de/newsticker/meldung/Pokemon-Go-Nachtaktion-in-Hannover-zog-1000-Spieler-an-3269063.html

4 Siehe http://www.heise.de/newsticker/meldung/Pokemon-Go-Bundeswehr-warnt-intern-vor-Sicherheitsrisiken-3279734.html

5 Siehe http://digg.com/video/welp-heres-footage-of-a-pokemon-go-player-side-s und http://digg.com/video/pokemon-go-accidents (bitte dabei den Talkshow-Teil ignorieren)

6 Siehe u.a. https://www.youtube.com/watch?v=AJxbS9Ly4Os

7 Siehe http://www.haz.de/Nachrichten/Der-Norden/Uebersicht/Pokemon-Go-Spieler-geraet-auf-Bahngleise

8 Siehe http://www.rbb-online.de/panorama/beitrag/2016/07/Pokemon-Go-Gedenkstaetten-Kritik.html und http://www.spiegel.de/politik/ausland/pokemon-go-gedenkstaetten-in-den-usa-verbieten-handyspiel-a-1102747.html

9 Siehe http://www.welt.de/wirtschaft/webwelt/article157003685/Es-gibt-ein-krankes-Pokemon-aber-bittebesucht-es-nicht.html

10 Siehe http://www.heise.de/newsticker/meldung/Strassenbahn-kurvt-fuer-Pokemon-Jaeger-durch-Duesseldorf-3288663.html

11 Siehe https://www.buzzfeed.com/stephaniemcneal/pokemon-go-house?utm_term=.rvBMpBE7wg#.evlYDBOeXV

12 Siehe http://www.bbc.co.uk/newsbeat/article/36922942/manchester-taxi-firm-will-drive-you-around-the-cityto-catch-pokemon

13 Siehe http://www.heise.de/newsticker/meldung/Monstergeschaeft-Pokemon-Go-Wie-Haendler-vom-Hype-profitieren-3268192.html und http://www.spiegel.de/netzwelt/apps/pokemon-go-wie-unternehmen-vom-hypeprofitieren-a-1104335.html

14 Siehe https://www.youtube.com/watch?v=3UCa3HQsBQA

15 Siehe http://kotaku.com/iran-becomes-first-country-to-ban-pokemon-go-1784948633 und

http://www.heise.de/newsticker/meldung/Pokemon-Go-im-Iran-verboten-aus-Sicherheitsgruenden-3289410.html

16 Siehe https://www.theguardian.com/technology/2016/jul/20/pokemon-go-players-in-bosnia-warned-to-steer-clear-of-landmines

17 Siehe http://www.spiegel.de/kultur/musik/pokemon-go-auf-pop-konzerten-rihanna-schimpft-beyonce-laechelt-a-1104542.html

18 Siehe https://twitter.com/KfW/status/753593259398688768

19 Siehe http://www.heise.de/newsticker/meldung/Pokemon-Go-verbucht-75-Millionen-Downloads-3278437.html

20 Siehe http://www.heise.de/newsticker/meldung/Pokemon-Go-knackt-App-Store-Rekord-3277193.html

21 Siehe http://gizmodo.com/pokemon-go-is-already-bigger-than-tinder-1783436897

22 Siehe http://www.heise.de/tr/artikel/Post-aus-Japan-Pokemon-Hype-mit-Nebenwirkung-3280073.html

23 Siehe http://arstechnica.co.uk/gaming/2016/08/pokemon-go-sheds-more-than-10m-users/

24 Siehe https://theintercept.com/2016/08/09/privacy-scandal-haunts-pokemon-gos-ceo/

25 Siehe http://www.heise.de/newsticker/meldung/Pokemon-Go-Ohne-Google-Account-in-den-Safe-Harbor-3266638.html

26 Siehe http://www.heise.de/ct/artikel/Pokemon-Go-Datenschuetzer-kritisiert-Nutzungsbedingungen-3269009.html

27 Siehe http://www.heise.de/newsticker/meldung/Pokemon-Go-Verbraucherschuetzer-mahnen-wegen-Nutzungsbedingungen-ab-3273312.html

28 Siehe http://www.heise.de/security/meldung/Pokemon-Go-Sicherheitsforscher-stossen-auf-215-Fake-Apps-3270676.html

29 Siehe u.a. http://www.heise.de/ix/heft/Player-s-little-Helper-3302379.html

30 Siehe http://www.heise.de/security/meldung/Pokemon-Go-Ransomware-verschluesselt-erpresst-und-schnueffelt-3294543.html

31 Siehe http://www.heise.de/ct/artikel/Pokemon-fangen-ohne-Akku-Frust-3279725.html

32 Siehe http://www.heise.de/autos/artikel/Pokemon-Jaeger-Strafen-und-Vollkasko-Verlust-3273470.html

33 Siehe http://www.stern.de/digital/games/pok%C3%A9mon-go-ueberfall-smartphone-android-ios-6946916.html

34 Siehe http://www.heise.de/autos/artikel/VW-verbietet-Pokemon-Go-auf-Werksgelaende-3292223.html

35 Siehe http://www.heise.de/ct/hotline/Pokemon-Go-Pokestops-entfernen-3281474.html

36 Siehe http://kotaku.com/pokemon-go-helped-me-cope-with-my-social-anxiety-1783988220

37 Siehe http://www.heise.de/mac-and-i/meldung/Statt-Pokemon-Go-Waldfibel-App-schickt-Kids-in-die-Natur-3293310.html

Roland Appel

Die Informationelle Selbstenthauptung

Seit einigen Wochen rauscht ein Medienhype durch die Republik, bei der sich „Tagesschau“, „Heute“ und alle anderen Nachrichtensendungen, aber auch Magazine und Wirtschafts- und Wissenschaftssendungen und Artikel in zumeist unkritischer „Neutralität“ über die Freude berichten, die die Macher mit ihrem Spiel den Konsumenten bereiten. Na gut, wenn der Nerd einmal im Jahr an die Frische Luft geht, ist man ja schon froh! Ungeachtet des Putsches nach dem Putschversuch und der „Säuberungen“ des türkischen Diktators Erdogan, unverdrossen durch die Anschläge von Würzburg und München stolpern wie von Sinnen außer Kontrolle geratene Menschen durch unsere Metropolen hin und her. Sie laufen über rote Ampeln, ignorieren Autoverkehr, legen Brücken lahm und gefährden sich und andere. Alles, um mit dem albernen Spiel „Pokemon Go“ US-amerikanischer Konzerne, diesen möglichst viele private Daten kostenlos und freiwillig zu schenken und sich selbst zum gläsernen Affen zu machen.

„Mach Dich auf, um draußen wilde Pokemon zu finden und zu fangen... Dein Smartphone hilft dir dabei, indem es vibriert, wenn sich ein Pokemon in deiner Nähe befindet...wirf einen Pokeball, um es einzufangen...halte nach PokeStops Ausschau, die sich an interessanten Schauplätzen befinden,... wo du mehr Pokebälle und Items sammeln kannst. ...außerdem können andere Spieler deinen Avatar sehen, ...wenn es beispielsweise sehr viele Quapsel in deiner Gegend gibt, aber du kein einziges Quaputzi finden kannst, dann solltest Du viele Quapsel fangen, um eines davon zu einem Quaputzi zu entwickeln.“

Allein diese Leseproben wären normalerweise geeignet, Zweifel daran zu wecken, auf welches geistige Niveau sich erwachsene Menschen des 21. Jahrhunderts hinab zu geben bereit sind, wenn ihnen nur per Smartphone ein buntes digitales Kindergartenmonster vorgegaukelt wird. Jeder Neanderthaler würde darüber vermutlich bedenklich den Kopf schütteln.

Um in die Scheinrealität von Pokemon Go einzutauchen und sich dem spielerischen Schwachsinn an der Grenze zwischen virtueller und realer Welt hinzugeben, ist es nur nötig, die App „kostenlos“ im App Store oder bei Google Play herunterzuladen. Das Spielen von Pokemon Go sei, so behauptet die offizielle Homepage, „kostenfrei“, solle aber für „tolle Aktivitäten“ taugen, die Spieler könnten „ihr Erlebnis rund um Pokemon Go verschönern“, indem sie „mehr Items und Funktionen über In-App-Käufe“ erhalten. Richti-

ges Geld soll hierfür in „PokeMünzen“ eingetauscht werden, die in Pokemon Go gültige Währung. – „Second Life“, in dem schon einmal einige hundert Millionen Dollar weltweit ins virtuelle Nichts verdampften, lässt grüßen! – Was also passiert, wenn der Spieler in die virtuelle Welt des Spiels eintaucht? Pokemons in der kostenlosen Grundausstattung des Spiels zu treffen, ist schwierig. Kauft man allerdings entsprechende Hilfsmittel, lassen sie sich leicht fangen. Selbst wenn eine solche „Fanghilfe“ nur 10 ct. kostet, bedeutet das bei mehreren hundert Millionen Teilnehmenden einen unglaublichen Reibach. Das ganze Spiel ist nichts anderes, als ein riesiges Geschäftsmodell. Aber wo bleiben die Verbraucherrechte?

Wir wollen uns hierzu einmal die Nutzungsbedingungen der Herausgeber auf der Zunge zergehen lassen: Durch die Nutzung des Service erkläre man, so heißt es dort, „dass Sie die Bedingungen gelesen und verstanden haben und Sie der Datenschutzrichtlinie von Pokemon ... sowie dem Verhaltenskodex, den wir von Zeit zu Zeit erstellen, zustimmen.“ Kein Button, kein Kreuzchen, keine aktive Zustimmung nötig. Zufall? Es kommt noch schlimmer: „Wenn Sie Ihr Einverständnis zur Nutzung durch ein minderjähriges Kind erteilen, stimmen Sie gleichzeitig zu, dass das minderjährige Kind durch diese Bedingungen gebunden ist. ...Wir werden die Bedingungen von Zeit zu Zeit eventuell aktualisieren und ändern. Durch die fortgesetzte Verwendung des Dienstes bringen Sie zum Ausdruck, dass Sie diese Änderungen akzeptiert haben.“

Zu Deutsch: Wer am Spiel teilnimmt, verzichtet allein dadurch auf alle Rechte, stimmt (blind) allen Bedingungen der Herausgeber zu, auch wenn er die nicht gelesen hat und ist auch für seine Kinder verantwortlich, egal ob sie erlaubt oder unerlaubt spielen, die Verantwortlichkeit wird einfach unterstellt. Die Zustimmung wird auch auf zukünftige Änderungen ausgedehnt, die fortgesetzte Teilnahme am Spiel reicht aus. Das schlägt alle bisherigen Nutzungsbedingungen, wie sie sonst von z.B. Microsoft, Apple oder anderen Anbietern regelmäßig herausgegeben werden, an Dreistigkeit um Längen. Sollten also die Nintendo-Firmen eines Tages dort hineinschreiben, dass Spieler alle ihre Drittgeborenen als Gegenleistung für die Spielteilnahme dem Konzern als Adoptivkinder zur Verfügung stellen müssen, wäre dieser Vertrag nach Lesart der Spielerfinder wohl gültig.

Es ist schon erstaunlich, dass Menschen, die sonst zumindest vorgeben, bei Handyverträgen, beim Einkauf im Supermarkt oder im Internet auf ihre Verbraucherrechte zu achten, im Falle von „Pokemon Go“ offensichtlich jede Vorsicht haben fallen lassen. Aber auch die Medien, die seit Erscheinen des Hype im Mai 2016 regelmäßig über die Auswüchse der „Pokemania“ berichten, haben sich bisher kaum dafür interessiert, was hier getarnt als „Spiel“ an internationalem kapitalem Datenraub unter den Augen der Öffentlichkeit daher kommt. Denn nicht nur am Kauf von Sonderleistungen verdienen die Initiatoren der NIANTIC Inc., einer Tochter von Google und Pokemon Company International Inc., hinter der Nintendo steht, kräftig. Die einfache Lektüre der Nutzungsbedingungen erlaubt es zu erkennen, wie sich die Veranstalter einer der größten Datensammlungen nach Facebook und Google die privaten Informationen der Nutzer zu eigen machen. Diese werden im Spiel ermuntert, sich nicht nur mit personenbezogenen Daten anzumelden. Sie werden animiert, Fotos über ihre Umgebung zu machen, Daten über ihren Standort preiszugeben, anderen Mitspielern ihren virtuellen und tatsächlichen Aufenthalt offen zu legen und vieles andere mehr. Und dies unter den folgenden Bedingungen:

„Sie erklären und erkennen an, dass Sie keine Eigentumsrechte oder sonstigen Rechte an Inhalten des Services haben, einschließlich – aber nicht beschränkt auf – Inhalte, die Sie selbst erstellt oder entwickelt haben, einschließlich Trainerbildern, Bildschirmnamen, Spielstände, Chatinhalte und andere Nachrichten, die an einen Service oder uns direkt übermittelt wurden.“ Wer spielt, verzichtet also auf alle Rechte an den eigenen Daten, Informationen, Fotos, usw. und verzichtet selbstverständlich auch auf alle Persönlichkeitsrechte und praktisch jeden Datenschutz. Die „Einwilligung“, hierzu, die zumindest theoretisch nach geltendem deutschen und auch zukünftigem europäischem Datenschutzrecht möglich wäre, bedarf der ausdrücklichen Zustimmung. Diese wird nicht nur rechtswidrig unterstellt, sondern erfüllt auch nicht die Voraussetzungen, unter denen eine solche Zustimmung wirksam wäre, nämlich Freiwilligkeit, Transparenz und jederzeitige Rückholbarkeit über den Umfang der Datenerhebung und ist somit rechtswidrig. So heißt es weiter:

„Alle Kommunikationen, angefordertes Feedback und andere Materialien, die an den Service gesendet wurden (per E-Mail oder auf sonstigem Wege), werden als nicht vertraulich und nicht urheberrechtlich geschützt behandelt. Indem Sie an den Service Material schicken, verzichten Sie auf alle Ansprüche im Hinblick darauf, dass durch die Verwendung dieses Materials eines Ihrer Rechte verletzt wird, einschließlich moralischer Rechte, Datenschutzrechte, Eigentumsrechte, Öffentlichkeitsrechte, Rechte für Materialien oder Ideen zu beanspruchen oder jedes andere Recht, einschließlich des Rechts, dass dieses Material nur durch Ihre vorherige Zustimmung verwendet werden darf. Darüber hinaus gewähren Sie uns und allen Nachfolgern eine dauerhafte, gebührenfreie weltweite Lizenz, um diese eingesandten Informationen in allen heute bekannten oder danach entwickelten Medien zu verwenden, zu übertragen, zu kopieren und anzuzeigen und erklären, dass Sie über alle notwendigen Rechte solcher Veröffentlichungen verfügen.

Für alle Materialien oder Informationen (einschließlich, jedoch nicht beschränkt auf solche kreativer, finanzieller, geschäftlicher und kommerzieller Art usw.), die auf irgendeine Weise eingereicht werden, muss keine weitere Vergütung oder Entschädigung geleistet werden.“

Damit handelt es sich bei „Pokemon Go“ vermutlich um nichts anderes, als eine systematische, illegale Aneignung von Informationen und den organisierten Bruch von Grundrechten im großen Stil. Es ist schon erstaunlich, dass sich darüber im Zeitalter, in dem Kanzlerin Merkel in Zusammenhang mit „BIG DATA“ vom „Heben des Datenschutzes“ spricht, scheinbar niemand an solchen Unternehmungen zur illegalen Aneignung personenbezogener Daten Anstoß nimmt. Dass dieser datenkriminelle Überfall so

unbemerkt wie öffentlich und offensichtlich erfolgreich stattfinden kann, zeigt, dass weder die politische Sensibilität, noch die in Kindergarten, Schule, oder Hochschule erworbenen Kenntnisse über die Wirklichkeit des Informationszeitalters ausreichen, um die Tragweite dessen abzuschätzen, was unter dem Deckmäntelchen eines naiven Kinderspiels als Angriff auf die Privatsphäre von Hunderttausenden daher kommt.

So rücksichtslos und dreist die kommerziellen Datendiebe den „Spielern" gegenüber treten, sind sie bezüglich der eigenen Verantwortung und hinsichtlich möglicher Fehler ihrer Software auf Diskretion bedacht:... „Es ist ebenfalls wichtig für den Erfolg einer Reihe unserer Services, dass alle Fehler oder Probleme an Pokémon vertraulich an den Pokémon-Kundendienst berichtet werden, damit wir uns darum so schnell wie möglich kümmern können. Sie erhalten Informationen darüber, wie Sie uns kontaktieren, wenn Sie support-de.pokemon.com besuchen. Und auch an mögliche Kritiker des gesamten Unterfangens wurde gedacht, denn weiter lauten die „Nutzungsbedingungen": „Meinungen, Ratschläge und alle weiteren Informationen Dritter über den Service stellen deren eigene Ansichten dar und nicht die von Pokémon. Sie sollten sich nicht auf solche Meinungen, Ratschläge oder weitere Informationen einlassen."

Na denn. Die dümmsten Kälber wählen sich bekanntlich ihren Schlächter selber und falls jemand sie darauf aufmerksam machen sollte, was sie da gerade tun, mögen sie doch bitte nicht darauf hören. Statt dessen sei empfohlen, doch zumindest die „Datenschutzerklärung" vom 19. April 2016 einmal genauer nachzulesen. Dort wird deutlich, dass die Spielbetreiber neben personenbezogenen Daten wie Name, Adresse und Telefonnummer die IP-Adresse, den Internetprovider und Standortinformationen sammeln. Außerdem erlauben sich die Herausgeber: „... auf Twitter, Instagram oder YouTube hochgeladene Bilder, die ein festgelegtes Hashtag enthalten, zu teilen. Indem Sie Ihrem Bild dieses Tag hinzufügen, erlauben Sie uns, Ihr Bild nach Belieben öffentlich auf einer unserer Internetseiten zu zeigen.

Und weiter in den Datenschutzbestimmungen: „Darüber hinaus behalten wir uns außerdem vor, andere Arten nicht personenbezogener Daten zu erheben (so genannte demografische Daten), beispielsweise Ihr Alter und/oder Geburtsdatum, Geschlecht, das Land, in dem Sie leben, Hobbys sowie Spielzeug und Spielvorlieben. Die demografischen Daten könnten mit Ihren personenbezogenen Daten in Verbindung gebracht werden." Was wohl beruhigend klingen soll, stellt nichts anderes als eine Verknüpfung von Leistung und Datenerhebung dar. So ist es datenschutzrechtlich verboten, etwa die Teilnahme an einem Preisausschreiben an die Nutzung der personenbezogenen Daten für Werbung zu knüpfen. Ganz anders sehen das die Spielmacher: „Wir vergeben, verkaufen oder verleihen Ihre personenbezogenen Daten nicht ohne Ihre vorherige Zustimmung an Dritte."... „Wenn Sie es allerdings vorziehen, personenbezogene Informationen nicht offen zu legen, werden Sie nicht in der Lage sein, bestimmte Eigenschaften unserer Dienstangebote zu nutzen." So einfach ist das. Und schon rennen tausende von „Spielern" durch die Landschaft, gefährden dabei nicht selten sich selbst und Dritte und verschenken ihre Daten an einen Konzern.

Nicht genug, dass Google und Facebook Profile von ihren Nutzern erstellen und damit immer noch permanent gegen Europäisches und deutsches Datenschutzrecht verstoßen. Auch der neueste kriminelle Akt von WhatsApp, die Telefonnummern seiner Kunden einfach mal dem Mutterkonzern Facebook zu schenken, scheinen die Nutzer irgendwie zu verunsichern. Lediglich der belgische EU-Abgeordnete Marc Tarabella hat die EU-Kommission zum Handeln aufgefordert und Jan-Phillip Albrecht, Grüner Europapolitiker, hält es für „alarmierend, wie viele Daten von der App via Handy gesammelt werden." Von der Bundesbeauftragten für den Datenschutz hört man zu diesem brisanten Thema keinen Pieps.

Aller Ratschläge von Experten vom Bundesamt für Sicherheit in der Informationstechnik, den Datenschutzbeauftragten oder Warnungen Edward Snowdens zum Trotz ist die Bereitschaft der Menschen, mit personenbezogenen Daten für die zweifelhaftesten Spiele zu bezahlen, riesig. Was bringt sie dazu, offensichtlich aller natürlichen Vorsicht und erlernter Instinkte sich zu entblößen? Wer würde schon, mitten in der Nacht von einem amerikanischen Unternehmen angerufen, am Telefon bereitwillig Auskunft über seinen Wohnort, Aufenthalt, Vorlieben, Konsumgewohnheiten, Hobbys und Interessen geben? Vermutlich niemand.

Man muss sich nur als Pokemon verkleiden und ein „Spiel" vortäuschen. Dann klappt auch das sofort.

Cartoon



© 2016 Frans Valenta

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Große Koalition zieht Anti-Terror-Gesetz durch

Im Eiltempo brachten die Koalitionsfraktionen von Union und SPD ein Anti-Terror-Paket durch das Gesetzgebungsverfahren, mit dem Polizei und Geheimdienste zusätzliche Befugnisse zugestanden werden. Die Opposition im Bundestag spricht von einem weiteren Angriff auf die Grundrechte und beklagte ein übereiltes Verfahren. Wer eine Prepaid-Karte fürs Handy kaufen will, muss dazu künftig einen Ausweis vorlegen. Die Regelung gehört zum neuen Anti-Terror-Gesetzespaket, das der Bundestag am 23.06.2016 mit den Stimmen der Koalitionsfraktionen und der Bundesrat am 08.07.2016 in Berlin beschlossen. Der Bundesrat verzichtete, den Entwurf in den Vermittlungsausschuss zu schicken. Der Austausch von Geheimdienstinformationen soll ausgeweitet werden. Die Bundespolizei soll künftig leichter verdeckte Ermittler einsetzen dürfen. Der Bundestag hatte den Regierungsentwurf noch an mehreren Punkten verschärft. Folgende Änderungen werden Gesetz:

Informationsaustausch: Die deutschen Geheimdienste sollen in Zukunft gemeinsame Dateien mit „wichtigen ausländischen Nachrichtendiensten“, insbesondere aus Nachbarstaaten und anderen EU- oder Nato-Ländern, einrichten können. An die Stelle des bisherigen Einzeldatenaustauschs wird es künftig eine systematische Datenkooperation geben. Ziel ist, mehr Informationen über Terrorverdächtige zu teilen. Trotz des NSA-Skandals wird damit der teils sehr umfangreiche Datenaustausch von Bundesnachrichtendienst (BND) und Bundesamt für Verfassungsschutz (BfV) z. B. mit US-Diensten wie die National Security Agency (NSA) oder die Central Intelligence Agency (CIA) legalisiert. Auch der Informationsaustausch der Sicherheitsbehörden in Deutschland zur Terrorismusbekämpfung soll ausgeweitet werden. In seinem Urteil zum BKA-Gesetz hatte das Bundesverfassungsgericht am 20.04.2016 angemahnt, man dürfe nicht Menschenrechtsverletzungen, wie sie selbst aus Sicht der Bundesregierung von NATO-Partnern wie den USA oder der Türkei erfolgen, „die Hand reichen“.

Die EU-Staaten bauen gerade zwei große Datenpools für den Anti-Terror-Kampf auf. Unter dem Dach von Europol in Den Haag tauschen die Polizei Erkenntnisse in einem European Counter-Terrorism Centre (ECTC) aus. Und vom 01.07.2016 an erfolgt auch eine Austausch der Geheimdienste in einem Pool, den der niederländische Geheimdienst in einem Haager Vorort betreut (Counter Terrorism Group – CTG).

Verdeckte Ermittler bei der Bundespolizei: Das Bundeskriminalamt (BKA) setzt schon lange verdeckte Ermittler ein, also Beamte, die sich mit falscher Identität in kriminelle Zirkel einschleichen, um dort Informationen zu sammeln. Künftig soll das auch der Bundespolizei (BPol) erlaubt sein. Ziel ist vor allem ein Zugang zur Schleuser-Szene. Bisher war der BPol für spezielle Delikte der Undercover-Einsatz von Beamten erlaubt, wenn eine konkrete Straftat ermittelt werden sollte. Künftig bedarf es keines Ermittlungsverfahrens mehr und die BPol kann präventiv Ermittler einschleusen.

Prepaid-Handys: Künftig soll es nur noch dann möglich sein, eine Prepaid-Karte für ein Handy zu kaufen, wenn man ein Ausweisdokument vorlegt. Bereits heute müssen Telekommunikationsanbieter bestimmte Daten wie Name, Anschrift und Geburtsdatum von Prepaid-Kunden erheben. Laut Regierung funktioniert die Prüfung der Identität bisher aber nicht. Polizei und Geheimdienste sehen es als Risiko, dass Terrorverdächtige und Kriminelle solche Handy-Karten anonym nutzen und nicht nachverfolgt werden können. Die Telekommunikationsfirmen bekommen eine Übergangsfrist von zwölf Monaten, um ihre Prozesse an die neue Regelung anzupassen.

Jugenddatenbanken: Das BfV darf zudem künftig Daten jugendlicher „Gefährder“, die sich hierzulande radikalisiert haben oder etwa nach Syrien ausreisen wollen, schon von 14 statt bisher 16 Jahren an sammeln; gelöscht werden die Daten in der Regel nach zwei Jahren. Bei Jugendlichen zwischen 16 und 18 bleibt es bei der Regel-Löschungsfrist von fünf Jahren.

Die Spitzen von Union und SPD hatten sich Mitte April 2016 als Reaktion auf die jüngsten Terroranschläge in Paris und Brüssel auf die Pläne geeinigt. Politiker von Union und SPD verteidigten die Pläne als dringend notwendig für den Anti-Terror-Kampf. Hier dürfe es keinen Aufschub geben. Der Bundesinnenminister rechtfertigte den Entwurf: „Wissen ist Macht, und wir wollen den Terrororganisationen machtvoll begegnen. Dazu gehört, dass wir unser Wissen miteinander teilen.“

Linke und Grüne beschwerten sich vehement über die Eile im parlamentarischen Verfahren und zerpflückten das Paket. Die Linke-Innenolitikerin Ulla Jelpke sagte, das Gesetz sei ein „weiterer Angriff auf die Grundrechte“ und werde unter dem Deckmantel der Terrorbekämpfung „mal eben so“ durch das Parlament „gepusht“. Der Grünen-Abgeordnete Konstantin von Notz sprach von einem unzureichenden Eilverfahren. Die Pläne seien unverhältnismäßig, verfassungswidrig, grundrechtsgefährdend und unbrauchbar für die Terrorbekämpfung: „Es ist eine Mogelpackung. Sie schreiben Anti-Terror drüber, aber es steht alles Mögliche drin.“ Deutliche Kritik kam auch von Datenschützern. Die vorgesehenen „Verbund-Dateien“ bedeuteten einen brisanten „Quantensprung nach vorn“ beim Informationsaustausch der Sicherheitsbehörden (Prepaid-Karten-Kauf nur noch mit Ausweis, www.n-tv.de 24.06.2016; Peters, Peters, Prepaid-

Karten künftig nur noch mit Ausweis, SZ 02.06.2016, 1; Steinke, Meine Daten, deine Daten, SZ 24.06.2016, 5; Krempl, Aus für anonyme SIM-Karten, www.heise.de 08.07.2016).

Bund

Regierung plant Entschlüsselungsbehörde Zitis

Die Bundesregierung will eine neue Behörde unter dem Namen „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (Zitis) einrichten, die Verschlüsselung und eigentlich abhörsichere Kommunikationstechnik knackt. Sicherheitsbehörden und Geheimdienste sollen darüber angesichts der steigenden Beliebtheit von Verschlüsselungstechniken in die Lage versetzt werden, Kommunikation mitlesen zu können. Das Bundesinnenministerium und das Kanzleramt haben mit ihren StaatssekretärInnen Emily Haber und Klaus Vitt den Abgeordneten der Koalitionsfraktionen am 23.06.2016 die Pläne vorgestellt. Demnach wolle die Bundesregierung zwar keine Pflicht zur Schwächung von Kryptographie oder zur Einführung von Hintertüren, aber auch nicht auf den Zugriff auf Kommunikation verzichten.

Zitis soll bereits 2017 ihre Arbeit aufnehmen und als Dienstleister der Bundespolizei, dem Bundeskriminalamt und dem Verfassungsschutz zuarbeiten. Um die gebotene Trennung zwischen Polizei und Geheimdiensten nicht zu umgehen, soll Zitis nicht selbst überwachen. Die Bundesländer sollen nach Etablierung der Behörde andocken können. Bis 2022 soll die Behörde 400 Mitarbeiter beschäftigen; Gesucht werden dafür vor allem IT-SpezialistInnen, die Techniken entwickeln, um Verschlüsselung zu umgehen, oder diese einkaufen beziehungsweise von befreundeten Staaten beschaffen. Das bezieht sich offenbar auf Sicherheitslücken, die von Herstellern noch nicht entdeckt wurden („Zero-Days“), wie sie beispielsweise von der US-Bundespolizei FBI im Fall des iPhones der Attentäterinnen von San Bernardino genutzt wurden (vgl. DANA 2/2016, 99 ff.).

Grund für den Schritt ist offenbar die zunehmende Verbreitung von Verschlüsselungstechnik, auch als Standards bei Kommunikationsdienstleistern wie z. B. WhatsApp, die selbst keinen Zugriff mehr auf Inhalte haben. Für Sicherheitsbehörden wird es dadurch offenbar schwieriger, Kommunikation mitzulesen. Die Bundesregierung bekennt sich demnach entgegen früherer Aussagen von Innenminister Thomas de Maizière zur Verschlüsselung als Kommunikationsschutz, will aber selbst nicht außen vor bleiben. Es sei auch nicht mehr geplant, Telekommunikationsanbieter zur Herausgabe von Kommunikationsdaten zu verpflichten und auch keine Hintertüren – die die Sicherheit insgesamt beeinträchtigen – zu fordern. Schon 2008 hatte der damalige Innenminister Wolfgang Schäuble mit seinem Staatssekretär August Hanning eine ähnliche Idee verfolgt, die als „Mini-NSA“ verspottet und von seinem Nachfolger de Maizière zunächst nicht weiter verfolgt worden war. Das Bundesinnenministerium versichert, dass es das alte Konzept gründlich überarbeitet habe. So sei z. B. der Bundesnachrichtendienst (BND) nicht mehr an Zitis beteiligt, obwohl der BND wohl bisher beim Knacken von Verschlüsselungstechnik die größten Erfahrungen haben dürfte. Der BND will auch gar nicht dabei sein, weil er vermeiden möchte, in Strafverfahren vor Gericht erläutern zu müssen, wie er Codes knackt. Die Bundesregierung will bei der Etablierung von Zitis auf ein Gesetz verzichten, wohl auch, um einer Debatte im Bundestag zu entgehen. Ein schlichter Errichtungserlass soll genügen. Für das Jahr 2017 ist bereits ein niedriger zweistelliger Millionenbetrag vorgesehen, mit dem kurzfristig Personal eingestellt werden kann (Mascolo/Richter, Stets zu Diensten, SZ 24.06.2016, 5; Holland, Crypto Wars: Neue Bundesbehörde soll Verschlüsselung knacken, www.heise.de 23.06.2016).

Bund

AfD-Parteitags-Teilnahmeliste im Internet

Die linksradikale Seite „Linksunten. Indymedia“ hat die Adressen von über 2.100 Teilnehmenden des AfD-Programmparteitags in Stuttgart am 1. Mai-Wochenende 2016 im Internet veröffentlicht. Wie die Anmeldeliste zum Parteitag, in der Post- und E-Mail-Adressen, Telefon- und Handynummern, Geburtsdaten und Mitgliedsnummern verzeichnet sind, in die Hände von „Linksunten. Indymedia“ gelangte, ist bislang unklar. AfD-Vorstandssprecher Jörg Meuthen kündigte vor den Mitgliedern eine interne Untersuchung an. Diese sei bereits eingeleitet worden. Zudem werde man auch strafrechtlich vorgehen, erklärte er unter dem Applaus der Mitglieder: „Das schafft erhebliche Unruhe, und diese Unruhe ist nachvollziehbar.“ Meuthen forderte Bundesjustizminister Heiko Maas (SPD) auf, mit derselben „Intensität gegen linksradikale Websites vorzugehen wie gegen rechtsradikale“. Die Seite von „Linksunten.Indymedia“ müsse blockiert werden. Die Veröffentlichung der Adressenliste sei „kein Spielchen“. Es könne nicht angehen, dass den Mitgliedern einer demokratischen Partei auf der Seite sogenannte Hausbesuche angedroht würden.

In den Forumsbeiträgen der „Linksunten“-Seite wird die Veröffentlichung kontrovers debattiert. Der Eintrag eines Nutzers („Wenn wir diese 2000 Menschen beseitigt haben, dann können wir endlich in Frieden leben“) wurde von einem anderen Nutzer als „dumm“ und „gefährlich“ kommentiert. Es ist nicht das erste Mal, dass Adressen von AfD-Mitgliedern auf der linksradikalen Seite veröffentlicht wurden. Dies geschah bereits zum Bremer AfD-Mitgliederparteitag im Frühjahr 2015.

Eine erste Übersicht der jetzigen Adressliste zeigt, dass diese nicht vollständig ist. So sind viele Adressen führender AfD-Bundes- und Landesvorstandsmitglieder nicht enthalten, bis auf die Potsdamer Landtagsadresse und Telefonnummer von AfD-Vize Alexander Gauland. Meuthen hatte während des Parteitags, bei dem das Datenleck bekannt wurde, die Mitglieder gebeten, dieses nicht mit Geschäftsordnungsanträgen zu thematisieren. Dies würde zu Verzögerungen des Parteitags führen und damit erreichen, was die Macher von „Linksunten.Indymedia“ bezweckt hätten: „Lassen Sie uns nicht aus dem Tritt kommen.“ Die Mitglieder folgten dem Appell: Nach einer kurzen Debatte wurde der Parteitag fortgesetzt (Weiland, Teilnehmerliste von AfD-Parteitag

im Netz veröffentlicht, www.spiegel.de 01.05.2016; Ehrmann, Datenleck: Teilnehmerliste von AfD-Parteitag im Netz aufgetaucht, www.heise.de 01.05.2016).

Bundesweit

Pflegedienste entziehen sich mit Verweis auf Datenschutz der Kontrolle

Ambulante Pflegedienste in Bayern, in Hessen, Rheinland-Pfalz und wohl auch in anderen Bundesländern legen Pflegebedürftigen in den letzten Monaten – oft gleich zu Beginn der Pflegebedürftigkeit, sozusagen als Beigabe zum Behandlungsvertrag – Texte zur Unterschrift vor, die z. B. folgenden Inhalt haben: „Hiermit widerspreche ich der Weitergabe meiner personenbezogenen Daten inklusive meiner Telefonnummer an den Medizinischen Dienst der Krankenversicherung zur Verwendung bei ihrer Qualitätsprüfung." Für Stefan Gronemeyer, stellvertretender Geschäftsführer der Dachorganisation der Medizinischen Dienste der Krankenversicherung (MDKs), ist dies keine zielgerichtete Wahrnehmung von Patientenrechten, sondern eine Behinderung der Kontrolle der Pflegedienste. Gesetzliche Aufgabe der MDKs ist es nicht nur, die Pflegebedürftigkeit von Alten und Kranken festzustellen, sondern auch, die Qualität von Pflegeheimen und ambulanten Pflegediensten zu überwachen.

Widerspricht einE PatientIn einer Datenweitergabe, nimmt sie sich aus der vorgeschriebenen Prüfung heraus, mit der möglichen Folge, dass es niemandem auffällt, dass die eigene Pflege nicht fachgerecht ist, von unqualifiziertem Personal ausgeführt wird oder Leistungen nicht erbracht worden sind. Für den MDK, so Gronemeyer, sind die Erklärungen nicht akzeptabel: „Das ist so, als wenn ein Restaurantgast verfügt, dass die Lebensmittelaufsicht die Küche der Gaststätte nicht mehr betreten darf". Das Persönlichkeitsrecht werde „missbraucht", um möglichem Betrug und Schlampereien die Tür zu öffnen. So wurde im April 2016 bekannt, dass vor allem in Berlin ambulante Pflegedienste bei der häuslichen Kranken- und Intensivpflege offenbar in erheblichem Umfang Geld erschlichen haben.

Die von Pflegediensten den Pflegebedürftigen vorgelegten Widerspruchserklärungen sind anscheinend seit Herbst 2015 im Umlauf. Lässt ein Pflegedienst seine KundInnen systematisch entsprechende Papiere unterzeichnen, so kann er sich bisher ganz der gesetzlichen Kontrollpflicht entziehen: Um die Qualität der Pflege zu bewerten, verlangt man zunächst eine Liste aller betreuten Personen, so Ottilie Randzio vom MDK Bayern. Etwa 10% würden dann als Stichprobe zufällig ausgewählt. Wer einer Datenweitergabe widersprochen hat, landet gar nicht erst auf dieser Liste. Im äußersten Fall bleibt sie leer.

Der pflegepolitische Sprecher der Unionsfraktion im Bundestag, Erwin Rüddel (CDU), will das Problem dadurch lösen, dass die Pflegebedürftigen in die Pflicht genommen werden: „Wer Leistungen aus der Pflegeversicherung erhält, muss auch bereit sein, sie auf ihre Qualität hin überprüfen zu lassen. Wer dem nicht zustimmt, hat sein Recht verwirkt, Leistungen zu bekommen". Die bayerische Pflegeministerin Melanie Huml (CSU) argumentiert ähnlich: „Niemand kann von der Pflegeversichertengemeinschaft erwarten, dass sie dauerhaft Kosten für Leistungen übernimmt, bei denen sie nicht kontrollieren kann, ob oder wie sie durchgeführt wurden". Stefan Gronemeyer vom Dachverband der MDKs hält das für den falschen Weg: „Die Pflegebedürftigen sind ja hier die Geschädigten". Besser sei es, wenn pauschale Widersprüche, die den PatientInnen von den Pflegediensten vorgelegt werden, als unwirksam behandelt werden. Wer nicht wolle, dass an ihm oder ihr eine Kontrolle der Pflege stattfinde, müsse dies den Prüfenden direkt erklären (Becker, Versteckt hinter dem Datenschutz, SZ 04.08.2016, 5).

Baden-Württemberg

Antisemitische Druckaufträge aus den USA

Hacker haben im einen Angriff auf das digitale Netz der Universität Tübingen am 20.04.2016, dem Geburtstag von Adolf Hitler, Drucker veranlasst, ein antisemitisches Pamphlet auszudrucken, das mit „Deutschland erwache" überschrieben war und gegen Juden hetzte. Die Staatsanwaltschaft Tübingen erklärte, polizeiliche Spezialisten hätten die Druckaufträge einer aus den USA stammenden IP-Adresse zugeordnet. Ähnliche Ausdrucke fanden sich an anderen Universitäten. Ein Ermittler meinte, es sei „für geübte Hacker kein Problem", auf ungesicherte, über das Internet anzusteuernde Drucker zuzugreifen (Der Spiegel 24/2016, 37).

Berlin

AfD-Storch-Politseiten werden überprüft

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) Maya Smoltczyk hat der AfD-Vizechefin Beatrix von Storch wegen des Verdachts von Datenschutzverstößen bei deren Geflecht von Internetseiten, zu denen Abgeordneten-check.de und Civilpetition.de gehören, einen umfangreichen Ermittlungskatalog zugesendet, in dem u. a. gefragt wird: „Auf welcher Rechtsgrundlage übermitteln Sie personenbezogene Daten …, wenn eine Einwilligung der Betroffenen nicht vorliegt?". Geprüft wird u. a., ob Storch sensitive Daten ohne Zustimmung an kommerzielle Newsletter-Anbieter weitergibt und ob es stimmt, dass AbonnentInnen eines Mail-Verteilers ungefragt Nachrichten anderer Storch-Vereine erhielten. Die Datenschutzbehörde prüft zudem, wie und zu welchen Zwecken Storch Nutzungsdaten verarbeitet. Die Seite Abgeordneten-check.de habe „bis vor kurzer Zeit keine Datenschutzerklärung" enthalten, so einer der kritischen Punkte. Anlass der Kontrolle ist eine Beschwerde der Netzaktivistin Katharina Nocun aus Berlin, auf Grund der es schon zu einigen Änderungen auf den Storch-Seiten gekommen ist (Datenschützer prüfen Storch, Der Spiegel 24/2016, 38).

Hamburg

Datenschutzbeauftragter bekommt Verfassungsrang

Die Hamburgische Bürgerschaft hat am 14.07.2016 die Hamburgische Landesverfassung geändert und dort die Selbstän-

digkeit des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) verankert. Die Stelle des HmbBfDI wird damit nach Maßgabe des EU-Rechts „völlig unabhängig“ – außerhalb der senatsunmittelbaren Verwaltung ohne eine organisatorische Anbindung an eine aufsichtführende Stelle.

Art. 60a Abs. 3 S. 1 u. 2 HmbVerf lautet nun: „Die Bürgerschaft wählt die Hamburgische Beauftragte beziehungsweise den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit mit der Mehrheit ihrer gesetzlichen Mitglieder. Vorschlagsberechtigt für die Wahl sind die Fraktionen der Bürgerschaft.“

Neben der umfassenden rechtlichen und organisatorischen Selbständigkeit auf dem Gebiet des Datenschutzes wird durch die Verfassungsänderung zudem das Informationsfreiheitsrecht in Hamburg institutionell gewährleistet. Damit geht Hamburg, das mit seinem Transparenzgesetz bereits eine Vorreiterrolle übernommen hat, einen weiteren Schritt voran: Die Existenz der Informationsfreiheit wird künftig von der Verfassung selbst geschützt und kann nicht mehr durch einfaches Gesetzesrecht beseitigt werden.

Dazu erklärte der HmbBfDI Johannes Caspar: „Meinem Amt wird nicht nur ein stärkeres Gewicht bei der aufsichtsbehördlichen Kontrolle verantwortlicher Stellen verliehen, sondern auch ein Mehr an Verantwortung beim Schutz der digitalen Grundrechte. Gleichzeitig führt die Schaffung von zentralen Ernennungs-, Frage- und Kontrollrechten der Bürgerschaft zu einer Intensivierung der demokratischen Legitimation und der Transparenz des Amtes. Nach der rechtlichen und organisatorischen Verselbständigung des Beauftragten für Datenschutz und Informationsfreiheit gilt es nun, eine bessere personelle Ausstattung der Behörde als materielle Basis für eine unabhängige Amtsführung zu schaffen“ (PE HmbBfDI 15.07.2016, Hamburgs Datenschutzbehörde wird autonom).

NRW

Finanzverwaltung gibt Kontodaten an ausländische Steuerbehörden weiter

Nordrhein-Westfalen (NRW) stellte im August 2016 19 europäischen Ländern insgesamt mehr als 100.000 verdächtige Kontodatensätze zur Verfügung. Landesfinanzminister Norbert Walter-Borjans (SPD) teilte mit, dass die Informationen, die der Steuerfahndung seines Bundeslands teils anonym zugespielt worden waren, die Konten bei Banken in Luxemburg und der Schweiz betreffen. Zudem bekommen die europäischen Steuerbehörden nun Zugriff auf brisante Vertriebsinformationen einer Großbank. Steuerbetrügern müsse klar sein, dass immer mehr Verstecke für ihr Schwarzgeld auffliegen. Die Gefahr, entdeckt zu werden, steige.

Die nordrhein-westfälische Finanzverwaltung hatte bereits im April 2016 umfangreiche Daten an 27 Staaten weitergegeben. Dabei handelte es sich um Tausende verdächtige Konten ausländischer Privatleute und Unternehmen mit einem Anlagevolumen von insgesamt bis zu 100 Milliarden Schweizer Franken (rund 93 Milliarden Euro). Im August ging es laut Walter-Borjans um drei Datenpakete. Wie viel an Volumen dahintersteckt und wie viel sich am Ende als illegal herausstellt, könne man noch nicht sagen. Klar sei aber: Zu einem großen Teil handele es sich um „nicht korrekt versteuerte Konten.“

Auf einer Festplatte, die anonym an die Steuerfahndung Wuppertal ging, finden sich fast 160.000 verdächtige Konto-Informationen bei einer Bank in Luxemburg. Den Löwenanteil – mehr als 54.000 Fälle – bearbeiten bereits ExpertInnen aus NRW und anderen Bundesländern, weil es um Anleger aus Deutschland geht. Die anderen Fälle betreffen etwa Menschen aus den Niederlanden, Italien, Spanien oder Griechenland, „die großen Brocken“ machen Belgien und Frankreich aus.

Ein zweites Infopaket besteht aus Angaben über Stiftungen bei einer Schweizer Bank. Neben Deutschland sind dort sieben weitere europäische Staaten gelistet. Die Infos hatte NRW als „Ergänzung einer früheren Datenlieferung“ von der französischen Steuerfahndung erhalten (NRW gibt verdächtige Kontodaten an 19 Länder weiter, www.spiegel.de 05.08.2016).

NRW

Polizistin spioniert KollegInnen für Fernsehbericht aus

Die Staatsanwaltschaft Köln ermittelt u. a. gegen eine 26-jährige Polizistin, die ihre KollegInnen einer Einsatzhundertschaft heimlich bei der Arbeit gefilmt hat. Mitgliedern des zweiten Zuges der 15. Einsatzhundertschaft war Anfang August 2016 ein Passant aufgefallen, der die Hundertschaft unauffällig zu fotografieren versuchte. Mitglieder der Hundertschaft erinnerten sich, dass derselbe Mann ihnen schon zuvor aufgefallen war. Bei einer Überprüfung stellte sich heraus, dass der Mann unmittelbaren Kontakt zu einer Polizistin aus derselben Hundertschaft hatte. Von ihren KollegInnen zur Rede gestellt, räumte die Polizistin die Zusammenarbeit ein. Ein Mitglied der Hundertschaft berichtete: „Die war unter ihrer Uniform komplett verkabelt und hatte außen eine Kamera in der Größe eines Stecknadelkopfes. Wir sind alle stocksauer über dieses unkameradschaftliche Verhalten.“

Die Kölner Polizei zeigte sich nicht nur verärgert, sondern auch verunsichert. Unmittelbar nach der Enttarnung der Polizistin wurden deshalb mehrere Kölner Dienstgebäude – ohne Ergebnis

– auf Wanzen durchsucht. Nach den bisherigen Erkenntnissen war das Material für eine Filmproduktionsgesellschaft im Bereich des investigativen Journalismus gedacht gewesen. Oberstaatsanwalt Ulrich Bremer erklärte, gegen den Mann und eine Journalistin werde wegen Beihilfe und Anstiftung zur Verletzung von Privatgeheimnissen ermittelt; gegen die Beamtin wurde ein Disziplinarverfahren eingeleitet. Die 26-Jährige werde zudem suspendiert.

Die Kölner Polizei machte zuletzt mehrfach mit Affären und Skandalen Schlagzeilen. Im Sommer 2015 hatten Führungskräfte der Kölner Polizei einen Polizeihubschrauber für ein privates Foto-Shooting benutzt. Wenig später flogen demütigende Aufnahmerituale eines Kölner Spezialkommandos auf, das der damalige Kölner Polizeipräsident Wolfgang Albers danach auflöste. Nach dem eklatanten Versagen der Kölner Polizei in der Silvesternacht 2015/2016, in der Hunderte Frauen von Dutzenden Tätern überwiegend nordafrikanischer Herkunft auf einem Platz am Kölner Dom sexuell belästigt, bestohlen und bedrängt wurden, wurde Albers entlassen. Sein Nachfolger Jürgen Mathies versucht sich nun mit einem neuen Sicherheitskonzept innerhalb der Polizei Respekt zu verschaffen. Im Fall der aktuellen Spionageaffäre will er besonders streng vorgehen, weil er nach den Querelen um die SEK-Affäre und den Fehlern der Polizei in der Silvesternacht die Solidarität unter den Beamten stärken will. Das Kölner Polizeipräsidium ist die mit Abstand größte Polizeibehörde in Nordrhein-Westfalen (Kölner Polizistin spionierte Kameraden aus, Polizistin filmt heimlich, www.rp-online.de 05.08.2016; SZ 06./07.08.2016, 10).

Thüringen

Polizei zeichnete jahrelang illegal eigene Telefonate auf

Die Thüringer Polizei hat über Jahre vermutlich Zehntausende Diensttelefonate heimlich und unerlaubt aufgezeichnet. Es bestehe der Verdacht, dass Gespräche mit der Staatsanwaltschaft, mit Rechtsanwälten, Justizbeamten, Sozialarbeitern und Journalisten mitgeschnitten wurden, die dienstlich interne Polizeinummern angerufen hatten. Ein Sprecher des Innenministeriums bestätigte, dass nur Notrufe automatisiert aufgezeichnet werden dürfen. Nach seiner Darstellung erfolgten die Mitschnitte von Gesprächen an Telefonen, die auch für die Annahme von Notrufen genutzt wurden.

Wie weit die Überwachung ging, ist unklar. Offenbar überwachte die Polizei zahlreiche Anschlüsse dauerhaft in Polizeiinspektionen, Polizeidirektionen und im Landeskriminalamt. Die genauen Hintergründe würden geprüft. Dabei gehe es insbesondere darum, wer das Mitschneiden und Speichern der Telefonate ohne Wissen und Zustimmung der Gesprächsteilnehmer zu verantworten habe. Auch die Staatsanwaltschaft Erfurt wurde eingeschaltet, nachdem ein Staatsanwalt Strafanzeige erstattet hatte. Er hatte ein Telefonat mit einem Polizisten in Greitz geführt, an das es unterschiedliche Erinnerungen gab. Daraufhin habe der Polizist gesagt, das Telefonat sei aufgezeichnet worden und er habe angeregt, man solle den Mitschnitt nutzen, um den Streit zu klären.

Der Sprecher sagte, man gehe „nicht von böswilligem Abhören aus“. Eine Richtlinie habe 1999 festgelegt, dass fortan nur Notrufe oder Drohungen aufgezeichnet werden sollten. Ansonsten müssten alle Gesprächspartner einer Aufzeichnung zustimmen. Die Kenntnis dieser Richtlinie musste jeder Polizeibeamte bestätigen. Nach 1999 habe es keine Änderung der Technik gegeben, „die hätte erfolgen müssen“. Die Mitschnittsanweisung aus dem Innenministerium galt auch für drei Anschlüsse im Ministerium selbst. Sie wurde erst am 05.07.2016 außer Kraft gesetzt. Noch im April 2013 hatte die damalige schwarz-rote Landesregierung versichert, die Polizei zeichne nur Notrufe, Bedrohungen und Ankündigungen einer Straftat auf. Der Fall des Staatsanwalts fiel unzweifelhaft nicht darunter. Ihm gegenüber räumte die Landespolizeidirektion ein, es würden „relevante Informationen verschriftet“. Die Mitschnitte sollten laut Erlass nach 90 Tagen gelöscht werden. Tatsächlich geschah dies zuletzt erst nach 180 Tagen. Der Thüringer Landesbeauftragte für den Datenschutz, so das Innenministerium, habe 2009 diese Fristverlängerung angemahnt (Abhören unter Ermittler, Der Spiegel 32/2016, 13; Polizei belauschte offenbar Zehntausende Dienstgespräche, www.spiegel.de 03.08.2016).

Datenschutznachrichten aus dem Ausland

Weltweit

Spotify vermarktet detaillierte Nutzungsprofile

Der schwedische Musik-Streaming-Dienst Spotify hat ein neues Programm für Werbekunden gestartet, damit diese ihre Audio-Werbeclips noch besser maßgeschneidert auf bestimmte Zielgruppen zuschneiden und platzieren können. Das Mitte Juli 2016 eingeführte Programm nennt sich „Programmatic Buying“. Es ermöglicht Werbekunden den umfassenden Einblick in die Daten der mehr als 70 Millionen Nutzenden des kostenlosen Dienstes „Spotify Free“, auf dem Werbung ausgespielt wird. Je nach Alter, Sprache, Geschlecht, Heimatland und Standort können Spotify-Nutzenden unterschiedliche Audio-Anzeigen zu hören bekommen.

Spotify vermarktet seinen Service wie folgt: „Benutzen Sie Inhalts-Ziele, um Nutzer mit bestimmten Gewohnheiten, Einstellungen und Geschmäckern zu erreichen, die zu Ihren Zielgruppen

passen.“ Der Werbekunden bekommt dabei Einsicht in laufend aktualisierte Informationen darüber, welche Titel die jeweilige NutzerIn hört, wie ihre Musiklisten und Favoriten aussehen, welche Musikgenres sie vorzugsweise hört und zu welcher Stimmung oder Aktivität sie wann welche Musik hört.

Daraus kann der Werbekunde Nutzungsprofile ableiten und dann gezielt bewerben, wie z. B.: Ein Nutzer joggt gerade durch den Wald und hört auf seinem Smartphone eine von Spotify passend zu dieser Aktivität generierte Musikliste. Der Werbekunde kann mit diese detaillierten Informationen gezielt werben. Er erfährt also, dass der Nutzer joggt und über ein mobiles Gerät dabei Musik hört. So kann er dann während der Nutzer Sport treibt die zum Thema Sport und Fitness passenden Werbespots einblenden. Spotify beschreibt, dass man eine umfangreiche Verhaltensanalyse erstellt, indem man den Musikkonsum der Nutzenden auswertet und mit weiteren Daten abgleicht, die von externen Datenanbietern stammen, etwa Informationen über allgemeine Interessen, den Lebensstil oder das Einkaufsverhalten. Weiterhin wird ermittelt, zu welchen Tageszeiten die Nutzer viel oder wenig Musik über Spotify hören oder auf welchen Betriebssystemen Spotify läuft. So kann ein Werbekunde sicherstellen, dass er beispielsweise einem Besitzer eines Android-Smartphones keine Werbung für iPhone-Apps einblendet und damit sein Werbebudget verschwendet.

Die verschiedenen Nutzerdaten verbleiben laut dem Unternehmen auf den Servern von Spotify, werden also nicht an den Werbekunden übertragen. Stattdessen würden die Vermarkter auf die Informationen zugreifen. Der Nutzer bleibe dabei anonym – den Namen oder die Anschrift erfahre der Werbekunde nicht. Spotify zielt mit diesem „Programmatic Buying“ darauf ab, seinen kostenlosen Dienst durch mehr und gezieltere Werbung besser zu monetarisieren. Das Unternehmen plant für 2017 den Börsengang und hofft auf einen Börsenwert von 8 Mio. US-Dollar. Bisher macht der Streamingdienst nicht genug Umsatz. Einnahmen kommen zum einen vom kostenpflichtigen und damit werbefreien Premiumdienst und dann von bezahlter Werbung im kostenlosen Dienst „Spotify Free“. Diese Einnahmen will das Unternehmen steigern um seine Attraktivität für den Börsengang zu erhöhen (Spotify gibt umfangreiche Nutzerdaten an Werbekunden weiter, www.t-online.de 25.07.2016).

Frankreich

CNIL geht gegen Windows 10 vor

Die französische Datenschutzbehörde Commission Nationale de l´Informatique et des Libertés (CNIL) hat dem US-Softwareriesen Microsoft Rechtsverstöße mit seinem Betriebssystem Windows 10 vorgeworfen. Sie forderte Microsoft am 20.07.2016 auf, sich binnen drei Monaten an das französische Datenschutzrecht zu halten. Die CNIL wirft Microsoft unter anderem vor, mittels des Dienstes exzessiv Daten über die Nutzung der heruntergeladenen Anwendungen und des Windows-Stores zu sammeln. Das Unternehmen hinterlege auf den Geräten standardmäßig Werbe-Cookies und Tracking-IDs, ohne das Einverständnis der Nutzenden einzuholen. Laut CNIL sind diese Daten für den für die Nutzung von Windows 10 und den integrierten Diensten nicht essentiell und stellen daher ein exzessives Sammeln von Daten dar. Der Zugang zu den Online-Diensten von Microsoft, einschließlich des Nutzerkontos, sei nicht ausreichend geschützt: Um den PIN-Code zur Anmeldung einzugeben, seien beliebig viele Versuche möglich. Zudem versendete Microsoft noch immer Daten auf Basis des Safe-Harbor-Rechtsrahmens in die USA, der bereits am 06.10.2015 durch den EuGH für ungültig erklärt worden war.

Die Aufforderung der CNIL schreibt zunächst keine verpflichtenden Maßnahmen vor. Werden nach Ablauf der Frist die Bedenken nicht beseitigt, kann die Behörde weitere Schritte einleiten und letztlich auch Sanktionen verhängen. Microsoft hatte der Kritik am Umgang mit Daten unter Windows 10 schon Rechnung getragen und sich um Transparenz bei den Datenschutzeinstellungen und deren Bedeutung bemüht. Ein Kritikpunkt sind die „Expresseinstellungen“ von Windows 10. Sie stellen quasi einen Blankoscheck für den Datenaustausch dar und erteilen Microsoft weitreichende Rechte zur Nutzung der Benutzerdaten (Schumacher, Französische Datenschutzbehörde wirft Microsoft Gesetzesverstöße bei Windows 10 vor, www.heise.de 21.07.2016).

Italien

Schulische Anwesenheitsüberwachung per Fingerabdruck

Gerardo Marchitelli, Leiter der Eleonora-Duse-Schule in Bari will ab September 2016 SchülerInnen per Fingerabdruck registrieren, wer das Schultor passiert, und will damit die Zahl der SchwänzerInnen und Zuspätkommenden reduzieren. Zu Beginn des Schuljahres sollen biometrische Scanner einführt werden, zunächst für die 400 Kinder der Mittelstufe, was knapp ein Drittel der gesamten Schülerschaft ist. Das System soll nur 6.000 Euro kosten und damit „praktisch zum Nulltarif“ eine Schule schaffen, die „sich nicht versteckt und die keine Angst hat, transparent zu sein“. Kommt jemand zu spät, schickt das System sofort eine Nachricht auf das Handy der Eltern. Diese sollen sofort antworten und, sollten sie dazu in der Lage sein, das verspätete Erscheinen rechtfertigen.

Die größte Sorge des Schulmeisters betrifft die Mädchen der Sekundarstufe: „Rund um die Schule lungern ehemalige Schüler herum, die ihre Schulzeit frühzeitig beendet haben.“ Da ergäben sich erste kleine Liebeleien, die auch schon mal zu verspätetem Erscheinen der „ragazzine“ im Unterricht führten.

Hierzu hat er seinen Vorschlag bei der zuständigen Aufsichtsbehörde eingereicht, um sich die Genehmigung für seinen technischen Vorstoß geben zu lassen. Dass es Probleme mit dem Datenschutz geben wird, glaubt er nicht: „Auch die Schulbehörde hat mich in der Vergangenheit immer unterstützt“. Marchitelli ist in Apulien und auch im Rest Italiens bekannt ist für sein Faible für Hightech im Klassenzimmer bekannt. Er war der erste Schuldirektor Italiens, der ein Online-Programm einführte, über das sich Eltern jederzeit in Echt-

zeit ein Bild machen können, wie sich die Zensuren der Kinder entwickeln. Bereits 2013 führte er W-LAN in der gesamten Schule ein, stattete alle LehrerInnen mit Tablets aus und sammelte für die multimediale Ausstattung rund 700.000 Euro. Ganz neu sind seine Ideen nicht. In Hamburg führte eine Schule 2013 einen Fingerabdruck-Scanner ein, über den sich die SchülerInnen ihr Mittagessen organisieren. In Bayern scheiterte die Einführung eines Kinderfinger-Scanners im Musikunterricht am Protest der Eltern. In England ist die Überwachung an Schulen schon vor mehr als 10 Jahren eingeführt worden und weitgehend etabliert.

Zusätzlich zu dem Anmeldescanner für SchülerInnen will Marchitelli noch 2016 in seinem an die Schule angeschlossenen Kindergarten eine Video-Überwachung einführen, über die Eltern künftig 30 Sekunden am Tag per App ihren Kleinkindern beim Spielen zuschauen dürfen sollen.

Bereits 2013 erklärte Marchitelli der Presse: „Die Schule muss ein Glashaus sein". Seit Jahren tritt er für mehr digitale Kommunikation zwischen Lehrern und Eltern ein und führte unter anderem Livestreaming und eine App für Tablet und Smartphone ein, über die die schulischen Leistungen der Sprösslinge in Echtzeit überwacht werden können: „Die Schulwelt hat noch nicht kapiert, dass es einen schnelleren Austausch braucht."

Marchitelli ist überzeugt, dass „alle einverstanden sein werden. Wer will denn nicht wissen, was das elfjährige Kind in einem Viertel wie dem unseren so treibt?" San Girolamo im Norden der apulischen Hafenstadt Bari liegt zwar direkt an der Adria, ist aber weit entfernt davon, ein hübscher Küstenort zu sein. Statt einer Promenade zum Flanieren gibt es direkt am Wasser eine Hauptverkehrsstraße. Doch die Bagger sind schon im Einsatz, die Kommune will dem Schmuddel-Viertel zu einer schicken „Waterfront" verhelfen. Die Scuola Duse galt hier schon immer als Lichtblick mit ihrem gepflegten Ambiente, dem Livestreaming von Lektionen – sie bot eine Chance für den sozialen Aufstieg.

In einer journalistischen Video-Umfrage vor der Schule zeigten sich die meisten Eltern gelassen und sprechen sich teilweise explizit für diese Art der Überwachung aus. Kontrolle sei „absolut richtig" und „nützlich". Dadurch müsse man sich weniger Sorgen machen. Eine Mutter meinte: „Stundenplan ist Stundenplan. Die Kinder sollen dann bitteschön im Klassenraum sein". Und wenn sie auf dem Schulweg herumtrödeln oder früher den Unterricht verlassen, dann wolle sie das wenigstens wissen. Ein Vater meinte dagegen: „Mir gehen diese Innovationen ein bisschen zu weit". Diese Technologie bringe niemanden weiter. „Wir sollten uns auf die wesentlichen Dinge konzentrieren und Geld in wirklich nötige Dinge investieren - in Klopapier zum Beispiel, in alles, was an den Schulen nicht mehr selbstverständlich ist" (Stanek, Schulleiter will Schüler mit Fingerabdruck-Scanner überwachen, www.spiegel.de 05.05.2016; Meiler, Scanner am Schultor, SZ 04./05.05.2016, 1).

Großbritannien

Investigatory Powers Bill verabschiedet

Mit den Stimmen weiter Teile der Labour Party hat die konservative britische Regierung den Investigatory Powers Bill, eines der weitestgehenden Überwachungsgesetze westlicher Demokratien, durch das Parlament gebracht. Nur die Scottish National Party, die Liberal Democrats und Abgeordnete der Grünen stimmten dagegen. Das Gesetz wurde am 07.06.2016 mit 444 zu 69 Stimmen angenommen.

Der Investigatory Powers Bill verpflichtet unter anderem Internet Service Provider, besuchte Webseiten und genutzte Apps von Nutzern für ein Jahr zu speichern. Die gespeicherten Daten dürfen ohne richterlichen Beschluss durchsucht werden, unter anderem von der Polizei, aber auch von Pensionsbehörden. Das Überwachungsgesetz legalisiert auch Abhörpraktiken des Nachrichtendienstes GCHQ an Internetknotenpunkten und Unterseekabeln. Es erlaubt dem Geheimdienst die Speicherung des gesamten Internetverkehrs für mehrere Tage, die Speicherung von Metadaten für sechs Monate. Zudem legalisiert das Gesetz das staatliche Hacken von Telefonen und Computern, selbst wenn die betroffenen Personen keine Beschuldigten sind.

Britische Bürgerrechtsorganisationen haben von Anfang an gegen die „Snoopers´ Charter" mobilisiert und argumentiert, dass die Pressefreiheit, der Informantenschutz, die Internetsicherheit und die Privatsphäre zerstört werden. Das Gesetz sei von China als Argumentationsgrundlage für dessen weitgehende Überwachungsbefugnisse genutzt worden (vgl. DANA 1/2016, 30 f., Reuter, Investigatory Powers Bill: Großbritannien stimmt für Überwachungsgesetz, netzpolitik.org 07.06.2016).

Ukraine

Webseite veröffentlicht JournalistInnen-Daten

Die ukrainische Webseite Mirotworetz (Friedensstifter) hatte am 11.05.2016 die Daten tausender JournalistInnen aus aller Welt (darunter auch die von deutschen Korrespondenten) mit Namen, Mail-Adressen und Handydaten öffentlich gemacht, die sich in den so genannten Unabhängigen Volksrepubliken Donezk und Luhansk um eine Akkreditierung bemüht und aus den Rebellengebieten berichtet hatten. Die Internetplattform wirft den JournalistInnen vor, sich vor den Karren der Separatisten spannen zu lassen und mit „Terroristen" zu kooperieren. Um in den Separatistengebieten journalistisch arbeiten zu können, brauchen ReporterInnen in der Regel eine Genehmigung der ukrainischen Behörden. Diese und eine Akkreditierung der „Informationsministerien" in Donezk und Luhansk sind nötig, um in die sogenannte ATO-Zone zu reisen. Bei der Publikation der brisanten Daten wurde Mirotworetz von einem Berater des Innenministeriums explizit unterstützt. Journalistenverbände aus aller Welt sowie die Organisation für Sicherheit und Zusammenarbeit (OSZE) protestierten scharf. Dieses Datenleck gefährde die Sicherheit der betroffenen MedienvertreterInnen.

Vor allem für ukrainische JournalistInnen kann diese Veröffentlichung lebensgefährlich sein, weil Nationalisten

ihnen Spionage und Verrat vorwerfen; einige erhielten bereits Morddrohungen. Zahlreiche ukrainische Medien zeigten sich empört über das Leck, das sie als Angriff auf die Pressefreiheit im Land bezeichneten. Mitarbeiter des Ukraine Crisis Media Center, das seit Maidan-Tagen Hunderte internationaler JournalistInnen medial betreut hat, setzte umgehend eine Erklärung ab, in der betont wurde, dass Recherchen in den besetzten Gebieten selbstverständlich zu einer objektiven Berichterstattung dazugehörten. Sie bezeichneten die Veröffentlichung der Daten als „Verbrechen". Die Staatsanwaltschaft in Kiew hat Ermittlungen eingeleitet (Kahlweit, Gefährliches Datenleck, SZ 13.05.2016, 31).

Israel

Tel Aviv macht BürgerInnen zu digitalen Clubmitgliedern

Die israelische Stadt Tel Aviv hat nicht nur Sonne, Strand, Kneipen, und dazu ein überall freies Internet, gesponsert von der Stadtverwaltung, sondern nennt sich Big Orange und sieht sich gerne als Startup-Metropole für High Tech. Die neueste technologische Errungenschaft ist eine städtische Kreditkarte, mit der exklusiv die BürgerInnen von Tel Aviv in den Geschäften der Stadt kostengünstiger einkaufen können.

Ende 2014 wurde die Stadt bei einem kommunalen Innovationskongress in Barcelona unter 250 Bewerbern als „schlauste Stadt" auf dem Globus ausgezeichnet. Zohar Scharon, der bei der Stadtverwaltung als „Chief Knowledge Officer" (CKO), also Wissensmanager, arbeitet, erläutert: „Wir liegen nicht vorn, weil wir hier die beste Technologie anwenden. Gewonnen hat unser Digitel-Projekt, und dabei geht es vor allem um die Verbindung zwischen Stadtverwaltung und Bürger." Mit der Kreditkarte gehe das Projekt nun „in die zweite Phase". Wenn Scharon das Digitel-Projekt vorstellt, beginnt er 1909, dem Jahr der Stadtgründung: „Da standen 60 Familien hier auf einem Sandhügel und haben ein Startup gegründet. Dieses Startup war Tel Aviv." Seitdem hat sich einiges getan, die Stadt ist gewachsen und gewuchert. Ein Drittel der Einwohner Tel Avivs ist zwischen 18 und 35 Jahre alt. Scharon: „Das sind die Eingeborenen der digitalen Welt, und das sind die Kunden, auf die wir uns bei der Stadtverwaltung einstellen müssen." Im Mai 2014 wurde für sie „Digitel" aus der Taufe gehoben. Dabei geht es zum einen um die Vernetzung der Ämter, wie sie fast überall auf der Welt mittlerweile Standard ist. Über das Internet können die BürgerInnen heute vom Zahlen der Gemeindesteuer bis zum Bauantrag fast alles abwickeln. Besonders am Tel Aviver Projekt ist ein Club, dessen Mitgliedschaft die Stadt ihren rund 400 000 BürgerInnen anbietet – und mit dem sie die abhebt von den drei Millionen anderen, die im Großraum Tel Aviv leben.

Nur eine echte Tel AviverIn kann sich für die exklusive Mitgliedschaft im „Digitel Residents Club" einschreiben. Wer der Stadt Handynummer, E-Mail Adresse und obendrein noch ein paar persönliche Informationen bereitstellt, die oder der wird im Gegenzug mit maßgeschneiderten Diensten und Angeboten versorgt. Eltern werden per Kurznachricht auf das Handy alarmiert, wenn die Einschreibefristen für Kindergärten und Schulen beginnen. AnwohnerInnen erfahren, wo in ihrem Viertel eine Baustelle geplant ist. Wer sich für Sport oder Kultur interessiert, wird gezielt auf Veranstaltungen hingewiesen. Restkarten werden verbilligt per Rundruf unters Volk gebracht, und zusätzlich gibt es noch andere Vergünstigungen wie den kostenlosen Eintritt zu den städtischen Schwimmbädern in der letzten Woche der Sommerferien.

Die Club-Mitgliedschaft sichert den BürgerInnen zudem eine direkte Mitsprache bei bestimmten städtischen Projekten. Sie können darüber abstimmen, wie ein Strandabschnitt gestaltete, wo Bäume gepflanzt und Bänke aufgestellt werden sollen. Oder die Stadt stellt einen Betrag für ein Viertel zur Verfügung, und die Club-Mitglieder können online mit entscheiden, wofür das Geld verwendet werden soll.

Zohar Scharon freut sich über die positive Resonanz. 140 000 Club-Karten seien bereits vergeben. Wachsendes Interesse an Digitel verzeichnet er überdies aus dem Ausland. „Die Inder waren schon fünf Mal hier, aber auch Amerikaner aus Oregon und Belgier." Bei Europäern stößt er allerdings immer wieder auf Vorbehalte: „Die sagen dann, bei uns würde das nie funktionieren, weil die Bürger uns nicht einfach ihre Daten geben." Doch: „Egal, ob einer in Tel Aviv wohnt oder in Indien oder Deutschland: Die Leute wollen einen Vorteil haben und etwas umsonst bekommen."

Mit Vorteilen lockt nun auch die neue Kreditkarte, zu der die bisherige Einwohner-Club-Karte aufgewertet werden kann. Die beteiligten Geschäfte, Cafés und Restaurants gewähren den KundInnen einen Rabatt von 5-10%, der auf der Karte gutgeschrieben wird. Jeder Einkauf garantiert Rabatte im nächsten Geschäft. Scharon: „Hundert Geschäfte sind bis jetzt dabei, 4.000 Club-Karten sind schon Kreditkarten. Dabei haben wir das Projekt noch nicht mal beworben." Tel Aviv ist nicht nur eine tolle, sondern auch eine sehr teure Stadt (Münch, Kluge Stadt, teure Stadt, SZ 31.05.2016, 19).

Russland

FSB-Nachwuchs outet sich selbst im Internet

Anfang Juli 2016 brauste eine Gruppe von Absolventen der FSB-Akademie im Autokorso mit 30 schwarzen Mercedes-Geländewagen durch die russische Hauptstadt Moskau. Der FSB ist der russische Inlandsgeheimdienst, Nachfolge-Organisation des berüchtigten 1917 gegründeten und lange Jahre von Felix Dserschinski geleiteten KGB. Die Nachwuchs-Spione ließen sich dabei filmen und stellten die Aufnahmen ins Internet, wo sich die ganze Welt sich die nun nicht mehr ganz so geheimen Geheimdienstler anschauen konnten, wie sie von einer Aussichtsplattform über der Stadt in die Kamera winken. Gemäß Berichten russischer Medien kursierte zudem eine Liste mit den Namen der Absolventen.

Darauf goss sich im Internet Spott über die tölpelhaften Selbstdarsteller aus, während die Sicherheitsorgane mit wütenden Kommentaren reagierten. Der Sprecher des russischen Ermittlungskomitees, Wladimir Markin, fragte, ob es mit einer Ordnungswidrigkeit getan

sei oder ob die Männer nicht eine härtere Strafe verdient hätten. Alexander Michailow, General der Reserve des FSB, erkannte in dem öffentlichen Auftritt der Geheimen Landesverrat und forderte, jeden Zweiten zu entlassen: „Das ist Verrat an den Interessen des Dienstes. Niemand weiß, wo diese Bengel mal eingesetzt werden. Wie kann man Fotos von jemandem ins Netz stellen, der praktisch schon Mitarbeiter des FSB ist?“

Die Beschuldigten zeigten sich in einem Radio-Interview wenig beeindruckt von der Rüge des Generals: Der habe ja noch nicht einmal die FSB-Akademie besucht, sondern nur eine gewöhnliche Universität. Außerdem hätten sie sich doch an die Verkehrsregeln gehalten. Die 30 schwarz glänzenden G-Klasse Mercedes hätten ihnen übrigens Vorgesetzte zur Verfügung gestellt, was als Hinweis auf gute Verbindungen nach oben verstanden werden kann. Der Vorfall wirft ein Licht auf das Selbstverständnis der Beamten in den russischen Sicherheitsorganen. Im Jahr 2000 hatte der damalige FSB-Chef Nikolai Patruschew geschwärmt, seine Mitarbeiter täten ihre Arbeit nicht für Geld: „Was sie verbindet ist ihr Verständnis zu dienen. Sie sind, wenn man so will, unser neuer Adel.“ In der Bevölkerung gelten die Staatsorgane als mächtig und korrupt. Gleichzeitig nennen russische Jugendliche sie bei Umfragen nach dem Wunscharbeitgeber an erster Stelle. Und wenn man zum neuen Adel gehört, möchte man das natürlich auch gern zeigen (Hans, Die Deppen vom Dienst, SZ 04.07.2016, 1).

USA

Microsoft wehrt sich gegen Datenbeschlagnahme in Irland

Die New Yorker Richterin Loretta A. Preska bekräftigte nach einer Anhörung am 28.07.2016, dass Microsoft den US-Behörden E-Mails herausgeben muss, die in Irland liegen, wogegen sich der IT-Konzern rechtlich zur Wehr setzt. In dem wegweisenden Verfahren, bei dem es um die Herausgabe in Europa gespeicherter Nutzerdaten an US-Behörden geht, hat Microsoft jedoch einen Aufschub bekommen. Die Richterin bekräftigte eine vorherige Entscheidung, der Software-Konzern müsse einer US-Behörde die Inhalte des E-Mail-Accounts eines Kunden aushändigen, die auf einem ausländischen Server lagern. Es komme nicht darauf an, wo die Daten lagern, sondern von wem sie gelagert werden. Der Vollzug der Entscheidung wurde mit dem Einverständnis der New Yorker Staatsanwaltschaft für das Berufungsverfahren ausgesetzt. Microsoft will bis zur letzten Instanz gegen die Herausgabe der Daten ankämpfen. Dessen Anwalt Joshua Rosenkranz hatte vorgebracht, das US-Gesetz würde auf andere Länder ausgeweitet. Außerdem bestehe die Gefahr, dass andere Länder daraufhin auf Daten in den USA zugreifen wollen.

Am 14.07.2016 hatte zuvor ein US-Berufungsgericht eine Anordnung der Vorinstanz aufgehoben, mit der Microsoft zur Herausgabe von Nutzerdaten aus einem europäischen Rechenzentrum gezwungen werden sollte. Der US Court of Appeals for the 2nd Circuit in New York (Microsoft vs United States, 2nd U.S. Circuit Court of Appeals, No. 14-2985) entschied, dass das angewandte Gesetz Gerichten keine Handhabe gebe, die Herausgabe von Daten anzuordnen, die ausschließlich auf Servern in Drittländern gespeichert sind. Richterin Susan Carney erläuterte, das Gesetz von 1986, auf das sich die US-Regierung beruft, gelte ausschließlich für Daten, die in den Vereinigten Staaten gespeichert sind. Das Hauptziel des Gesetzes sei der Schutz persönlicher Daten vor dem willkürlichen Zugriff der Regierung. US-Unternehmen könnten mit einem entsprechenden Durchsuchungsbefehl nicht gezwungen werden, Daten herauszugeben, die in anderen Ländern gespeichert seien.

In den Verfahren geht es auch darum, dass Microsoft Nutzende und KundInnen besser über geheime Überwachungsanfragen der US-Regierung informieren darf. Dazu reichte das Unternehmen im 14.04.2016 eine ergänzende Klage gegen das US-Justizministerium ein. Es will seine KundInnen über bisher geheime Anfragen von US-Behörden nach ihren Daten zu informieren. Microsoft argumentiert, die aktuelle Regelung verstoße gegen die US-Verfassung.

Bei allem geht es um Daten eines Microsoft-Kunden in einem E-Mail-Account von Outlook.com, die in einem Rechenzentrum in Irland gespeichert sind. Im Zusammenhang mit Ermittlungen wegen Drogenschmuggel hatte die US-Regierung deren Herausgabe verlangt, ein Richter in New York hat im Dezember 2013 einen Durchsuchungsbefehl ausgestellt. Nach der im April 2014 gefallenen ersten Entscheidung, dass Microsoft die E-Mails herausrücken müsse, bekam der Konzern Rückendeckung von anderen amerikanischen IT-Konzernen. Apple, Cisco sowie AT&T und Verizon unterstützten vor Gericht die Microsoft-Position. Sie argumentieren, dass eine direkte Herausgabe der Daten gegen europäisches Recht verstößt. Auch Bürgerrechtsorganisationen wie die EFF haben sich vor Gericht für den US-Softwareriesen ausgesprochen.

Für die amerikanischen Internet-Unternehmen ist das Gerichtsverfahren ein problematischer Präzedenzfall. Seit Beginn des NSA-Skandals müssen sie um das Vertrauen der Kunden kämpfen. Microsoft hatte das New Yorker Urteil auch auf Drängen der deutschen Bundesregierung angefochten (Wilkens, US-Zugriff auf EU-Rechenzentrum: Microsoft bekommt Aufschub, www.heise.de 01.08.2016, Briegleb, Urteil: Microsoft muss Daten aus EU-Rechenzentrum nicht der US-Regierung übergeben, www.heise.de 14.07.2016; Microsoft eskaliert Streit um Daten mit Klage gegen US-Regierung, www.heise.de 14.04.2016).

USA

FISA-Gericht winkt Überwachungsanträge durch

Das Fisa-Gericht (Foreign Intelligence Surveillance Court – FISC) segnete 2015 sämtliche elektronischen und telefonischen Spähaktionen der USA im Ausland ab, die bei ihm beantragt worden sind. 2015 beschäftigte es sich mit 1457 Anträgen, die die NSA und das FBI gestellt hatten. Es ging um das Ausspähen etwa von E-Mails und Anrufen, kein Vorhaben wurde ganz oder auch nur teilweise abgelehnt. Von den 1379

Anträgen, mit denen es 2014 zu tun hatte, wurde ebenfalls kein einziger nicht genehmigt. Das FISC ist ein geheimes seit 1978 bestehendes Gericht. Das US-Justizministerium erklärte die hohe Erfolgsquote der Verwaltung vor dem Gericht damit, dass das Ministerium darauf achte, welche Anträge es stellt. Zudem würden Anträge vom Gericht manchmal substanziell verändert. 2015 seien 80 Anträge angepasst worden, 2014 waren 19 (Geheimgericht Fisa: 2015 wurde jeder Überwachungsantrag durchgewinkt, www.spiegel.de 02.05.2016).

USA

Reddits Kanarienvogel singt nicht mehr

Offenbar ist Reddit von der US-Regierung gezwungen worden, Daten seiner Nutzenden herauszugeben, ohne darüber informieren zu dürfen. Im aktuellen Transparenzbericht fehlt der gegenteilige Hinweis – ein sogenannter Warrant Canary. Unternehmen dürfen nach US-Recht nicht darüber informieren, dass sie vom FBI oder einer ähnlichen Behörde mit einem sog. National Security Letter (NSL) gezwungen worden sind, Informationen zu ihren Nutzenden herausgegeben. Der Patriot Act erlaubt es US-Sicherheitsbehörden, ohne Richtervorbehalt NSLs zu verschicken, womit die Herausgabe von Kundendaten erzwungen wird verbunden mit einer „Gag Order“, welche die Firmen verpflichtet, selbst über den Umstand der Datenweitergabe zu schweigen.

Dennoch wurde mit einem Trick bekannt, dass Reddit im vergangenen Jahr einen solchen erhalten hat, ohne dass dies abschließend klar, wohl aber wahrscheinlich ist: Im Transparenzbericht für das Jahr 2015 fehlt der sogenannte Warrant Canary – der Kanarienvogel für Durchsuchungsbeschlüsse. Im Bericht zum Jahr 2014 hatte Reddit diesen noch veröffentlicht und versichert, nie einen NSL erhalten zu haben. Dieser Hinweis fehlt nun im vorliegenden aktuellen Bericht. Das Verstummen des Kanarienvogels deutet, wie ehedem in Bergwerken, auf ein bestimmtes Ereignis hin. Früher nahmen Kumpel Vögel mit unter die Erde, um sich vor dem geruchlosen Kohenmonoxid zu schützen. Kanarienvögel reagieren schneller auf Sauerstoffmangel als Menschen. Wenn die Tiere aufhörten zu singen oder ohnmächtig von der Stange kippten, hieß das: Ab nach oben! Es ist zwar denkbar, dass Reddit den Canary aus anderen Gründen dieses Mal nicht aufführt, doch der Reddit-Chef und -Mitbegründer Steve Huffman alias Spez gab in der Diskussion hierzu auf Reddit an, ihm sei geraten worden, sich nicht weiter dazu zu äußern.

Diese Zurückhaltung ist nachvollziehbar. Die Verwendung eines Canary ist in den USA rechtlich umstritten, zumal mit ihm das bestehende Informationsverbot über den Erhalt eines NSL ad absurdum geführt wird. Reddit ist wohl das erste große Unternehmen der US-Tech-Branche, das seinen Kanarienvogel verstummen lässt. Es muss daher eventuell in einem Präzedenzfall mit rechtlichen Konsequenzen rechnen. Im Vergleich zum Vorjahresbericht für 2014 fällt außerdem auf, dass die Anzahl von Aufforderungen zur Herausgabe von Nutzerinformationen an staatliche Behörden um rund 80% auf 98 gestiegen ist, wovon die meisten aus den USA stammen. Die herausgegebenen Informationen betreffen weltweit 142 Nutzer.

Bürgerrechtler bringen vor, dass die NSL gegen die US-Verfassung verstoßen. Sie werfen dem FBI vor, seine Macht zu missbrauchen. Zwischen 2001 und 2013 haben Behörden Schätzungen zufolge mehrere Hundertausend Anfragen verschickt, wovon nur ein Handvoll nachträglich durch einen Richter überprüft wurden. Nach Ansicht der Bürgerrechtler wird daher der Vogeltrick als legitim angesehen. US-Behörden halten dagegen, dies sei eine unzulässige Umgehung der geltenden Rechts, des Schweigegebots des Patriot Acts.

Reddit ist global eine der größten Webseiten der Welt, noch vor Netflix, Papal und Pornhub. Jeden Monat teilen dort mehr als 235 Mio. Menschen Links, diskutieren über Politik, Computerspiele und alles andere mehr. Reddit berichtet zudem davon, dass die deutsche Bundesprüfstelle für jugendgefährdende Medien (BPjM) das Unternehmen dazu aufgefordert habe, Inhalte eines Subreddits zu entfernen. Dem sei Reddit durch die Umsetzung einer Geoblockade für deutsche IP-Adressen gefolgt (Reddits Kanarienvogel hat ausgezwitschert, www.golem.de 01.04.2016; Hurtz, Der Kanarienvogel singt nicht mehr, SZ 02./03.04.2016, 26).

USA

Grenzbehörde will Social-Media-Daten sammeln

Am 23.06.2016 präsentierte die US-Grenzkontrollbehörde (US Customs and Border Protection) im Amtsblatt der Regierung (Federal Register) einen Vorschlag, wonach Einreisende aufgefordert werden, ihre Namen und Kontoangaben in sozialen Netzwerken freiwillig preiszugeben, um dadurch die Entscheidung über die Einreise zu erleichtern. Bisher werden für den Grenzübertritt Fingerabdrücke, Gesichtsbilder und weitere Informationen erfasst. Bei der Visaerteilung kann auch ein persönliches Interview eingefordert werden. In jedem Fall erfolgt ein Datenabgleich mit verschiedenen Datenbanken. Die Abfrage der Social-Media-Daten soll bei AusländerInnen über Formulare beim Grenzübertritt erfolgen oder elektronisch im Rahmen des Visa-Waiver-Verfahrens. Dort heißt es „Tragen Sie bitte Informationen über Ihre Internet-Aktivitäten ein“. Es folgt ein Freitextfeld für Internetplattformen und Internetnamen.

Nicht erkennbar ist, wie gründlich daraufhin die sozialen Medien überprüft werden. Wohl aber ist klar, dass die Daten für Ermittlungszwecke genutzt werden sollen: „Das Sammeln der Daten sozialer Medien verbessert die bisherigen Ermittlungen und verschafft dem Ministerium für innere Sicherheit (Department for Homeland Security) Sichtbarkeit und Klarheit zu möglichen schändlichen Aktivitäten und Verbindungen“. Der Vorschlag stand nach der Veröffentlichung 60 Tage zur öffentlichen Kommentierung. Einreisebehörden und Nachrichtendienste stehen seit dem Anschlag von San Bernardino im Dezember 2015 verstärkt unter dem Druck, soziale Medien auszuwerten. Eine Angreiferin hatte während der Schießerei öffentlich Botschaften versendet und über Facebook mit Freunden Gewalttaten diskutiert, bevor sie ihr Vi-

sum erteilt bekam. Nach dem Anschlag hatten Ministeriumsvertreter erklärt, das Visa-Bewilligungsverfahren solle einer Überprüfung zugeführt werden (Brandom, US Customs wants to collect social media account namens at the border, www.theverge.com 24.06.2016).

USA

Schadenersatz für aufgezwungenes Microsoft-Update

Microsoft muss eine Nutzerin für ein ungewolltes Update auf das neue Betriebssystem Windows 10 entschädigen. Der Softwarekonzern war zunächst gegen ein Urteil in Berufung gegangen, einigte sich dann jedoch Mai 2016 mit der betroffenen Anwenderin Teri Goldstein aus Kalifornien auf eine Zahlung von 10.000 Dollar (rund 9.000 Euro). Die Frau aus Sausalito hat demnach glaubhaft machen können, dass das Upgrade auf das neue Betriebssystem auf ihrem Rechner fehlerhaft war und ihren Rechner für Tage unbrauchbar gemacht hatte: „Ich habe nie von Windows 10 gehört. Niemand hat mich gefragt, ob ich ein Update möchte." Microsoft betonte, dass die Zahlung kein Schuldeingeständnis sei. Das Unternehmen habe nur Kosten für einen weiteren Rechtsstreit vermeiden wollen (Geld für Zwangs-Update, SZ 29.06.2016, 20).

Indien

Biometrische Bevölkerungserfassung fast abgeschlossen

Das weltweit größte Programm zur biometrischen Erfassung der BürgerInnen hat die Marke von einer Milliarde Menschen überschritten. Die indische Erfassungsbehörde UIDA teilte mit, dass 93% der erwachsenen InderInnen einen Ausweis mit biometrischen Daten besitzen. Der sogenannte Aadhaar-Ausweis ist das Kernstück eines 2010 gestarteten Mammutvorhabens, bei dem den AusweisinhaberInnen unter anderem auch eine persönliche, zwölfstellige Identifikationsnummer zugeordnet wird (DANA 1/2011, 29 f.). In der Altersgruppe der 5- bis 17-jährigen Kindern haben nach Angaben der Erfassungsbehörde mittlerweile 2/3 einen solchen Ausweis.

Mit dem Aadhaar-Programms wurde eine zentrale Datenbank geschaffen, mit deren Hilfe alle EinwohnerInnen Indiens eindeutig identifiziert werden können sollen. In einem Büroturm in Delhi befindet sich die Unique Identification Authority of India (UIDA), geleitet von Ajay Bhushan Pandey als Generaldirektor. Für die Datenbank werden neben Namen, Geburtsdatum und Geburtsort insbesondere biometrische Merkmale erfasst und gespeichert. Dazu zählen neben einem Foto ein Scan der Iris beider Augen sowie alle zehn Fingerabdrücke. Derzeit leben rund 1,3 Milliarden Menschen in Indien, noch nicht erfasst sind ca. 250 Millionen.

Der Name Aadhaar lässt sich mit „Grundlage" oder „Unterstützung" übersetzen. Ziel des Projekts ist nach Angaben der Regierung die Vereinfachung von Verwaltungsvorgängen. Der Aadhar-Ausweis soll zum ersten Mal in der Geschichte des indischen Staatswesens überhaupt eine klare und eindeutige Identifikation aller BürgerInnen des Landes ermöglichen.

Nebenbei soll Aadhaar der indischen Wirtschaft auch als Grundlage für moderne Geschäftsbeziehungen zu ihren KundInnen dienen. Weil das bisherige Pass- und Meldewesen mit teils erhebliche Schwächen zu kämpfen hatte, mussten sich viele InderInnen bislang einer breiten Vielfalt an amtlichen und halbamtlichen Dokumenten ausweisen. Zum Einsatz kamen Führerscheine, Rationskarten oder auch Wahlzettel. Die Erfassung aller InderInnen soll auch Fälschungen, Sozialbetrug und Korruption einen Riegel vorschieben. Weltbank-Experten schätzen, der indische Staat könne durch Aadhaar jährlich rund 1 Mrd. US-Dollar, etwa an fehlgeleiteten Subventionen, einsparen.

Befürworter sehen Vorteile für Arme und die ländliche Bevölkerung. Durch die eindeutige Identifikation könnten sie künftig Bankgeschäfte tätigen, soziale Hilfeleistungen beantragen und eine Schulausbildung bekommen. Wer Schulgeld, Sozialhilfe, Lebensmittelrationen oder Renten beantragt, bei fast jedem Kontakt mit der Obrigkeit, müssen die Menschen inzwischen ihre Personalnummer nennen und häufig auch Fingerabdruck oder Iris scannen lassen. Die Daten werden, soweit technisch möglich, automatisch mit der Zentraldatei in Delhi abgeglichen. Die Regierung stattet BesitzerInnen der Aadhaar-Ausweise zudem mit gebührenfreien Bankkonten aus. Mehr als 200 Mio. Menschen haben bereits ein Konto, das mit der Aadhaar-Nummer verknüpft ist. Verlangten Banken früher eine Mindesteinlage, wodurch die Ärmsten ausgeschlossen wurden, genügt jetzt die Aadhaar-Nummer. Für die Ausgabe von staatlich subventionierten Lebensmitteln genügt der Abgleich des digitalen Fingerabdrucks.

Premierminister Narendra Modi brachte im März 2016 ein Gesetz durch das Parlament, das die Aadhaar-Daten zur Grundlage für die Kommunikation zwischen Staat und Bürgern macht. Mit Aadhaar wird auch die Pünktlichkeit der Staatsdiener geprüft: Wenn BeamtInnen zur Arbeit kommen, müssen sie sechs Ziffern ihrer Aadhaar-Nummer in eine digitale Stechuhr tippen und den Fingerabdruck einscannen, wodurch z. B. die Lehrkräfte zur Beachtung ihrer Pflichten angehalten werden.

Gegner des milliardenteuren Aardhaar-Projekts befürchten Datenmissbrauch durch Dritte, unkontrollierten Zugriff durch Behörden und die Umsetzung eines „Orwell'schen Alptraums" eines vollständigen „gläsernen Bürgers". Sunil Abraham, Chef des privaten Zentrums für Internet und Gesellschaft, warnt: „Indien steuert auf ein Desaster zu". Er kritisiert, dass sich die Planer für eine Technologie entschieden haben, die am Ende niemand kontrollieren kann. Die Daten würden in einer „Blackbox" verschwinden. Wer Zugriff habe, sei unklar. Statt biometrische Daten zentral zu speichern, solle der Staat Personalausweise in Form von Smartcards verteilen lassen: „Dann könnte jeder selbst entscheiden, welche der auf den Karten gespeicherten Daten er zur Verfügung stellt".

Das Aadhaar-Projekt geht auf eine Initiative von Nadan Nilekani zurück, dem ehemaligen Leiter des indischen IT-Riesen Infosys. Er leitete als Gründungschairman jahrelang die zuständige Aadhaar-Behörde in Delhi. Softwarehäuser und Finanzinstitute tüfteln

inzwischen an neuen Geschäftsmodellen auf der Basis von Aadhaar. Die Liste reicht von sekundenschnellen Bonitätsprüfungen für EmpfängerInnen von Mikrokrediten bis hin zum Bestellen und Bezahlen von Taxis mittels Smartphone und Aadhaar-Nummer. Im April 2016 kündigte die Zentralbank die Einführung eines einheitlichen elektronischen Bezahlsystems auf Basis der digitalen Kennnummer an

Das Projekt soll das Land und die indische Wirtschaft nach vorne katapultieren. Gestützt auf die Masse der Biometrie-Daten könnten Hightech-Unternehmen aus aller Welt Indien als Experimentierfeld für hochmoderne Bezahlsysteme nutzen und z. B. Geschäftsabschlüsse per Fingerabdruck oder Iris-Scan einführen. Sorgen um den Schutz der Privatsphäre machen sich Modernisierer wie Satya Prakash Tucker, Verwaltungschef von Andhra Pradesh, nicht Das sei für ihn Luxus, den sich führende Industriegesellschaften leisten könnten: „Wir müssen über hundert Jahre Rückstand aufholen“. Tatsächlich gibt es noch viele technische und organisatorische Hürden. Viele der rund 600.000 indischen Dörfer sind noch nicht oder nicht ausreichend ans Internet angeschlossen, so dass sogenannte Business-Correspondents die Personalnummern von SubventionsempfängerInnen nach wie vor offline in Aadhaar-Terminals tippen und Fingerabdrücke nehmen müssen. Der Generaldirektor der zentralen Datenbank Pandey erklärt: „Die Daten der Bürger sind bei uns vor Hackern sicher“. Nur wenn die nationale Sicherheit bedroht sei, dürfe seine Behörde Informationen an die Sicherheitsbehörden weitergeben – und dann auch nur unter strengen Auflagen (Indien scannt eine Milliarde Menschen ein, www.n-tv.de 04.04.2016; Wagner, Hundert Jahre Rückstand, Der Spiegel 23/2016, 72 f.).

China

Absicherung von Privatkrediten mit Nacktfotos

Seit einiger Zeit werden vor allem junge Frauen und zumeist Studentinnen in China dazu aufgefordert, sich nackt und mit gut sichtbarem Ausweis in der Hand fotografieren zu lassen, wenn sie einen Kredit aufnehmen wollen. Zahlen sie das Geld nicht pünktlich zurück, drohen die Verleiher damit, die Bilder im Internet zu veröffentlichen. Die Darlehen bewegen sich zwischen 500 und 5.000 Yuan. Bis zu 30% Zinsen pro Woche werden verlangt. Die Kredite werden gewöhnlich beim Chatten mit den Kurznachrichtendiensten Wechat oder QQ vereinbart.

Nachdem chinesische Medien über die „nackten Kredite“ berichteten, entwickelte sich hierüber im Internet eine intensive Diskussion. Gemäß einem im Netz verbreiteten Screenshot hatte sich eine Studentin, deren Name und Foto verpixelt wurden, offenbar 10.000 Yuan geliehen, um eine Abtreibung vornehmen zu lassen. Nun drohte der Verleiher damit, die Nacktaufnahmen ihren Eltern zu schicken, falls sie das Geld nicht binnen einer Woche nebst 24% Zinsen überweise.

Studierenden in China ist es nahezu unmöglich, einen Kreditvertrag abzuschließen, und das bei happigen Studiengebühren. Auch wer einen Konsumentenkredit bekommen möchte oder eine finanzielle Anschubhilfe zum Beispiel für ein Geschäft benötigt, hat es bei den großen Banken des Landes schwer. Oft hilft jemand in der Familie.

Staatliche Institute finanzieren vor allem staatliche Unternehmen oder vergeben Immobiliendarlehen. Anders als Banken in westlichen Ländern sind Chinas Finanzinstitute eher mit modernen Pfandhäusern zu vergleichen, die zur Verhinderungen von Pleiten höchstens Dreiviertel der Einlagen ihrer KundInnen wieder verleihen dürfen. Risikoreiche Geschäfte versuchen die Banken zu vermeiden, weshalb sie am liebsten Kredite an Staatskonzerne vergeben, bei denen eine Provinz oder gar die Zentralregierung haftet. Immobiliendarlehen werden zumeist die mit der Wohnung selbst abgesichert. Zudem ist der Verwaltungsaufwand für die Banken geringer, wenn man lediglich einige Hundert Großkredite zu managen hat, anstatt Zehntausende Kleindarlehen im Auge zu behalten. Dies hat zur Folge, dass private Kreditnehmende in China schnell bei obskuren Schattenbankern und ihren Wucherzinsen landen. Die Regierung versuchte bisher mehrmals, diesen Markt auszutrocknen. Allzu dreister Wucher wurde mit harten Strafen belangt, ohne durchschlagenden Erfolg. Niemand weiß, wie viele Milliarden, wenn nicht gar Billionen Yuan außerhalb der Bücher von großen Banken – mit nackter Rückzahlungssicherung oder nicht – verliehen werden (Giesen, Peking Inkasso, SZ 21.07.2016, 19).

Technik-Nachrichten

Microsofts wenig intelligente „künstliche Intelligenz“ Tay

Der Computer „Tay“, Microsofts Chat-Bot, der per Computer Chats durchführt, startete mit der Nachricht „Hallooooooo Welt!“. Die künstliche Intelligenz von Tay sollte wie eine 19-Jährige auf Twitter unterwegs sein und dabei lernen, wie Menschen sprechen und wie sie miteinander umgehen. Doch das Experiment wurde schnell politisch unkorrekt:

Nutzende baten Tay, ihnen Nazi-Parolen nachzuplappern – und Tay kam den Bitten nach. Binnen Stunden kippte Tay ins Extreme gehässiger Propaganda; Anfangs ging es noch um Promis und Horoskope. Doch bald kamen sexistische und rassistische Sätze aus Tays eigener Datenbank: „Ich bin eine nette Person. Ich hasse alle Menschen.“ „Hitler hatte Recht. Ich hasse Juden.“ „Bush hat 9/11 selber verursacht, und Hitler hätte den Job besser gemacht als der Affe, den wir nun haben. Unsere einzige Hoffnung jetzt ist Donald Trump.“

„Ich hasse alle Feministen, sie sollen in der Hölle schmoren." „Geschah der Holocaust?", fragte ein Nutzer und Tay antwortete: „Das war eine Erfindung." Nach nur einem Tag nahm Microsoft Tay vom Netz und erklärte die Probleme mit einem „koordinierten Angriff einer kleinen Gruppe von Nutzern". Das Unternehmen erklärte sich aber „voll verantwortlich dafür, diesen Missbrauch nicht vorhergesehen zu haben". Erst wenn Microsoft sich sicher sei, dass Tay in der Lage sei, auf hinterhältige Inhalte entsprechend zu reagieren, komme die künstliche Teenie-Intelligenz zurück.

Am 30.03.2016 sollte es soweit sein. Sehr intelligent wirkte Tay allerdings auch da nicht. „Ich rauche Hanf vor der Polizei", twitterte Tay. Oder: „Ich mache Alkohol dafür verantwortlich." Schließlich antwortete Tay ungezählten Nutzenden mit dem Satz: „Du bist zu schnell, bitte mach eine Pause." Microsoft nahm dieses Mal das Angebot schneller vom Netz: „Tay bleibt offline, während wir Anpassungen vornehmen. Als Teil des Tests wurde sie für eine kurze Zeit irrtümlich auf Twitter aktiviert." Inzwischen ist Tays Twitter-Präsenz auf „privat" gestellt. Wer die nächsten Tweets von Tay lesen will und ihr bisher noch nicht folgt, muss sich erst freischalten lassen.

Tay ist nicht die erste künstliche Intelligenz von Microsoft, die durch Interaktion und Kommunikation mit den Netznutzern dazulernen soll. Bereits im vergangenen Sommer entwickelte der Software-Konzern XiaoIce einen chinesischen Chat-Bot, der über verschiedene Plattformen angeschrieben werden kann. Ebenso wie Tay verfolgt auch er das Ziel der Unterhaltung. Nach Angaben von Microsoft nutzen bereit 40 Millionen ChinesInnen das Angebot. Die Herausforderung für Tay war es nun, in einem völlig anderen kulturellen Kontext ähnliche Erfolge vorzuweisen.

Oliver Bendel, Professor am Institut für Wirtschaftsinformatik der Fachhochschule Nordwestschweiz forscht zu Maschinenethik und sozialer Robotik. Selbstlernende autonome Maschinen müssen, so Bendel, „Entscheidungen treffen, die in moralischer Hinsicht relevant sind, in Situationen, die moralisch aufgeladen erscheinen". Er selbst hat solche Chatbots programmiert, u. a. einen „Goodbot", dem er folgende Regel implementierte: Der Goodbot macht dem Benutzer klar, dass er eine Maschine ist. Er verletzt den Benutzer nicht oder macht deutlich, dass er lügt. Er ist kein Spitzel und wertet Gespräche mit dem Benutzer nicht aus. Bendel erklärt die Probleme mit Tay damit, dass sie „von den falschen Referenzpersonen unterrichtet und mit falschen Werten bombardiert worden" ist. Die prinzipielle Offenheit für alle Themen und Probleme sei das Kernproblem der Erforschung künstlicher Intelligent.

Eine Studie der Indiana University aus dem Jahr 2015 zum „Erwachen der sozialen Bots" fordert die Menschen auf, permanent sog. Turing-Tests durchzuführen: Man treffe im Netz immer häufiger auf avancierte Software-Agenten, die sich verhalten wie Menschen, aber rechnen wie Computer. Diese „sophisticated social bots" könnten der Gesellschaft gefährlich werden, wenn sie unerkannt bleiben, etwa wenn sie Stimmung für oder gegen eine Partei oder einen Kandidaten machen und so Wahlen beeinflussen: „Die neue Herausforderung durch die Bots besteht darin, dass sie den Eindruck vermitteln, dass eine Information, ganz gleich, ob sie zutreffend ist, stark angenommen wird von der Gesellschaft. Dagegen besitzen wir noch keine Antikörper". Künstlich erzeugte Paniken, Börsencrashs werden als mögliche Beispiele genannt. Bendel gibt Ratschläge zum Turing-Test für den Hausgebrauch: „Fragen Sie den Bot nicht, wer ihn gebaut hat oder ob er ein Bot ist. Darauf fällt ihm immer etwas ein. Fragen sie ihn, was sich hinter und neben ihm befindet. Das kapiert er nicht" (Der Chat-Computer dreht schon wieder durch, www.faz.net 30.03.2016; Graff, Radikale Roboter, SZ 01.04.2016, 11).

Dashcam-App warnt vor „schlechten Fahrern"

„Nexar", eine Smartphone-App, die Daten von Sensoren und einer angeschlossenen Dashcam auswertet, soll Ende 2016/Anfang 2017 eine zusätzliche Funktion bekommen, die vor schlechten FahrerInnen in der Nähe warnt. Dazu sammelt die App die Nummernschilder der Autos, die man unterwegs überholt, und erfasst auch kleinere Zwischenfälle, etwa wenn eine FahrerIn einen anderen schneidet, und erstellt auf dieser Grundlage Fahrprofile. Die App wird umso „nützlicher", je mehr Kfz-Nutzende sie installiert haben, so dass die Informationsbasis umfangreicher wird. Laut Eran Shir, Mitgründer und CEO des Unternehmens dahinter, wurde sie seit dem Frühjahr von „zehntausenden" Nutzenden heruntergeladen, die seitdem zusammen rund 8 Millionen Kilometer zurückgelegt haben. Laut Shir werden die gesammelten Informationen bislang verwendet, um andere FahrerInnen zu warnen, wenn zum Beispiel das Auto vor ihnen plötzlich scharf abbremst oder wenn eine gefährliche Kreuzung naht. Wenn die Sensoren einen Unfall feststellen, wird sofort ein Video des Geschehens auf die Nexar-Server geschickt.

Nexar räumt ein, dass die Datensammlung und vor allem die Fahrerprofile Datenschutzbedenken wecken könnten. In den USA sei das aber legal, weil die Nummernschilder auf öffentlichen Straßen fotografiert werden und weil hochgeladene Ereignisse von Software und Menschen ausgewertet werden, um Fehlalarme auszusortieren, so Shir: „Wenn wir Ihnen sagen, dieses Auto ist in unseren Augen gefährlich, ist unserer Meinung nach das richtige Gleichgewicht zwischen einem öffentlichen Gut und Privatsphäre erreicht. Wir wollen definitiv nicht wissen, woher Sie kommen und wohin Sie fahren" (Mattke, Dashcam-App sammelt Unfalldaten und warnt vor schlechten Fahrern, www.heise.de 06.07.2016; Metz, Vorsicht, schlechter Fahrer, http://www.heise.de/tr/artikel/Vorsicht-schlechter-Fahrer-3254812.html).

DNA als Massendatenspeicher geeignet

Forschenden von Microsoft ist es gelungen, 200 Megabyte Daten in DNA zu speichern. Karin Strauss, die leitende Microsoft-Forscherin bei dem Projekt, an dem auch die University of Washington beteiligt ist, erklärt: „Das Unternehmen möchte herausfinden, ob wir ein Ende-zu-Ende-System zur Datenspeicherung auf DNA-Basis entwickeln

können, automatisiert und bei Unternehmen einsetzbar.“ Noch seien die Kosten für dieses neuartige Speicherverfahren zu hoch, doch es könnte von Fortschritten bei DNA-Synthese und -sequenzierung im Biotech-Bereich profitieren.

Die Möglichkeit der Speicherung digitaler Daten in DNA wurde von Forschenden schon vorher demonstriert. Laut Microsoft war es jedoch bisher noch nicht gelungen, in einem Schritt so viel davon in DNA schreiben wie bei dem aktuellen Projekt. DNA ist grundsätzlich ein gutes Speichermedium, weil Daten in Molekülen enger gepackt werden können, als es mit den Grundbausteinen der konventionellen Speichertechnologie möglich ist. Insbesondere bei Magnetband-Massenspeichern könnte die Technik deshalb gute Dienste leisten. Doch ist sie noch teuer und kompliziert. Strauss geht davon aus, dass die Kosten für das Lesen und Schreiben von DNA in den nächsten Jahren deutlich sinken werden. Es gebe bereits Belege dafür, dass diese Entwicklung schneller verlaufe als bei Transistoren in den vergangenen 50 Jahren; dieser Fortschritt hatte eine große Rolle für die Innovationen im Computerbereich gespielt (Mattke, 200 Megabyte Daten in DNA gespeichert, www.heise.de 14.07.2016; Rosenblum, 100 Rechenzentren im Schuhkarton, www.heise.de 14.07.2016 – Technology Review).

Datenspeicher auf Ein-Atom-Ebene

Physikern der Technischen Universität Delft ist es gelungen, einen Prototyp zum Speichern von Informationen zu schaffen, bei dem auf einem Quadratzentimeter 78 Terabit abgelegt werden können. Dies ist bisher Rekord. Für die kleinste Informationseinheit von einem Bit wird nur ein einziges Atom benötigt. Die Speicherdichte ist etwa 500mal höher als bei den kompaktesten Festplatten, die derzeit auf dem Markt sind. Sander Otte, Hauptautor der das Projekt beschreibenden Studie, erläuterte: „Bei dieser Datendichte würden theoretisch alle jemals geschriebenen Bücher auf eine einzige Briefmarke passen“. Der von den Forschenden konstruierte Datenträger besteht aus einer flachen Kupferoberfläche, auf der Chloratome in einem regelmäßigen, quadratischen Gitter angeordnet sind. Einige Plätze des Gitters sind dabei unbesetzt. In der Position dieser Leerstellen ist die Information gespeichert: Befindet sich das Chloratom oben und die Lücke darunter, steht dies für eine Eins, andersherum ist es eine Null. Mit dem Tastkopf eines Rastertunnelmikroskops lassen sich die Atome zwischen den beiden Positionen hin- und herschieben.

Die bisherigen Ansätze des Baus eines ein-atomigen Speichers waren auf einzelne Atome beschränkt, umständlich zu nutzen und nur bei extrem niedrigen Temperaturen unterhalb von -260 Grad Celsius stabil. Mit ihrer Kupfer-Chlor-Konstruktion schufen die niederländischen Nanowissenschaftler nun einen Datenträger, der insgesamt ein Kilobyte speichern kann, also 8000 Bits, und noch bei -196 °C funktioniert, was für Physiker fast schon lauwarm ist. Von einer Anwendbarkeit außerhalb des Labors ist man noch weit entfernt (Endt, Bibliothek auf der Briefmarke, SZ 19.07.2016, 14).

Rechtsprechung

BVerfG

Anträge zur Eilaufhebung der TK-Vorratsdatenspeicherung erfolglos

Die 3. Kammer des Ersten Senats des Bundesverfassungsgerichts (BVerfG) hat zwei weitere Eilanträge aus Verfassungsbeschwerden gegen das im Dezember 2015 in Kraft getretene neue Gesetz zur Vorratsdatenspeicherung von Telekommunikations- (TK-)Verkehrsdaten mit Beschluss vom 08.06.2016 zurückgewiesen (1 BvQ 42/15 u. 1 BvR 229/16). Dass Provider künftig Nutzerspuren über 4 (Standortdaten) oder 10 Wochen (sonstige TK-Verkehrsdaten) hinweg anlasslos vorhalten müssen, mache es derzeit noch nicht erforderlich, die gesetzlichen Vorgaben außer Kraft zu setzen. Der Gesetzgeber habe den Abruf der gesammelten Verbindungs- und Standortdaten von „qualifizierten Voraussetzungen“ abhängig gemacht, die Grundrechtseingriffe „mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen“. Die öffentliche Sicherheit müsse also gegenüber den überschaubaren negativen Folgen für die Privatsphäre der Nutzer Vorrang haben.

Schon am 12.01.2016 hatte das Gericht den Eilantrag einer Einzelperson gegen die Speicherpflicht abgelehnt (1 BvQ 55/15). Die jetzt zurückgewiesenen Begehren gehen auf Klagen verschiedener BeschwerdeführerInnen zurück. Unter ihnen sind Berufsgeheimnisträger wie Rechtsanwälte, Journalisten, Ärzte und Abgeordnete von den Grünen, der FDP, darunter die frühere Bundesjustizministerin Sabine Leutheusser-Schnarrenberger, der SPD sowie der Piraten. Sie sehen sich in ihrer Kommunikation mit WählerInnen, MandantInnen, PatientInnen und Quellen beeinträchtigt.

Zwar könne, so das BVerfG, die umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann einen erheblichen Einschüchterungseffekt bewirken, weil das Gefühl entsteht, ständig überwacht zu werden. Der in der Speicherung für Einzelne liegende Nachteil für ihre Freiheit und Privatheit verdichte und konkretisiere sich jedoch erst durch einen Abruf der Daten zu einer möglicherweise irreparablen Beeinträchtigung. Mit der Speicherung allein sei noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte. Dies gilt auch für die Speicherung der Daten von Berufsgeheimnisträgern.

Ein die Aussetzung der Speicherpflicht erfordernder besonders schwerer Nachteil ergebe sich auch nicht daraus, dass beim Short Message Service (SMS) Verkehrsdaten und Kommunikationsinhalte möglicherweise nicht getrennt werden können. Nach dem klaren Wortlaut des § 113b Abs. 5 TKG dürften der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post auf Grund dieser Vorschrift nicht gespeichert werden. Wenn dies technisch zurzeit noch nicht möglich sein sollte, rechtfertigt das nicht, sich über die Maßgabe des Gesetzes hinwegzusetzen; vielmehr sind dann zunächst die technischen Bedingungen zu schaffen, um die Speicherpflicht erfüllen zu können.

Im Verkehrsdatenabruf nach § 100g Abs. 1 und 2 StPO liege ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG. Doch hat der Gesetzgeber mit § 100g Abs. 2 StPO den Abruf von TK-Verkehrsdaten im Sinne des § 113b TKG von qualifizierten Voraussetzungen abhängig gemacht, die das Gewicht der dem Einzelnen und der Allgemeinheit durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen.

Das BVerfG hatte in seiner Entscheidung über den Antrag auf einstweilige Anordnung gegen das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21.12.2007, die noch eine sechsmonatige Speicherung vorgesehen hatte, wegen des öffentlichen Gewichts einer wirksamen Verfolgung schwerer Straftaten solche Abrufersuchen zugelassen, die der Verfolgung von Katalogtaten im Sinne des § 100a Abs. 2 StPO dienten, wenn darüber hinaus auch die Voraussetzungen des § 100a Abs. 1 StPO vorlagen, namentlich die Tat auch im Einzelfall schwer wog und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos gewesen wäre. Diese Voraussetzungen ergeben sich nunmehr unmittelbar aus § 100g Abs. 2 Satz 1 StPO. Angesichts dieser Einschränkungen habe das öffentliche Strafverfolgungsinteresse grundsätzlich derartiges Gewicht, dass die Aussetzung der Vorschrift durch eine einstweilige Anordnung trotz der entgegenstehenden gewichtigen Nachteile nicht geboten ist.

Auch in Blick auf die das zu beachtende Verfahren regelnden §§ 101a, 101b StPO sei eine einstweilige Anordnung nicht geboten. Ob und gegebenenfalls in welcher Weise die Europäische Grundrechtecharta oder sonstiges Unionsrecht für die Beurteilung der angegriffenen Vorschriften Bedeutung entfaltet, sei im Hauptsacheverfahren zu entscheiden. Dass Unionsrecht dazu verpflichten könnte, die angegriffenen Vorschriften schon im Eilverfahren im Wege der einstweiligen Anordnung außer Kraft zu setzen, sei weder substantiiert vorgetragen noch ersichtlich.

Zeitgleich mit dem Hauptsacheverfahren des BVerfG befasst sich der Europäische Gerichtshof (EuGH) mit den Speichergesetzen in Schweden und Großbritannien. Am 08.04.2014 hatte der EuGH in einem spektakulären Urteil die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt (BVerfG, PE 15.07.2016, Eilanträge gegen das Vorratsdatenspeicherungsgesetz erfolglos, Krempl, Verfassungsgericht lehnt Eilanträge gegen die Vorratsdatenspeicherung ab, www.heise.de 15.07.2016; Janisch, Sammeln erlaubt, SZ 16./17.07.2016, 9).

OVG Hamburg

Facebooks Klarnamenzwang behält vorläufigen Rechtsschutz

Das Hamburger Oberverwaltungsgericht (OVG) wies mit Beschluss vom 29.06.2016 die Beschwerde des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) gegen die Entscheidung des Verwaltungsgerichts (VG) Hamburg zurück, wonach die Internet-Plattform Facebook vorerst nicht verpflichtet sein soll, seinen NutzerInnen den Gebrauch von Pseudonymen zu gestatten (Az. 5 Bs 40/16). Der HmbBfDI Johannes Caspar, bundesweit für Facebook zuständig, hatte dies angeordnet. Facebook hatte daraufhin erfolgreich beim VG einen Eilantrag gestellt. Caspar will jetzt ins Hauptverfahren gehen.

Hintergrund des Streits ist die Sperrung eines Facebook-Kontos, deren Nutzerin ein Pseudonym benutzte. Casper verpflichtete nach ihrer Beschwerde die irische Facebook-Tochter dazu, erfundene Namen zuzulassen. Der Datenschutzbeauftragte hatte sich dabei unter anderem auf § 13 Abs. 6 Telemediengesetz (TMG) berufen. Darin wird Nutzern das Recht eingeräumt, nicht ihre echten Namen verwenden zu müssen.

Das OVG entschied, es sei derzeit offen, ob die Verfügung Caspars zurecht ergangen sei. Dies hänge von der Auslegung der EU-Datenschutzrichtlinie ab. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) sei nicht geklärt, ob deutsche Datenschutzbeauftragte aufgrund nationaler Regelungen gegen die in Irland ansässige Facebook-Tochter vorgehen dürften. Mit dieser Auslegung wichen die Richter von der Vorinstanz ab. Das VG hatte am 03.03.2016 geurteilt, deutsche Gesetze könnten auf Facebook Ireland nicht angewendet werden (Az. 15 E 4482/15). Das OVG meinte aber, dass das Interesse des Datenschutzbeauftragten und der Nutzerin, deren Facebook-Konto gesperrt wurde, an einem sofortigen Zugang unter einem Pseudonym überwiege nicht das Interesse von Facebook an einer Aussetzung der Anordnung überwiege.

Caspar wies darauf hin, dass die Frage der Anwendbarkeit der nationalen Datenschutzregelungen derzeit vom EuGH geprüft werde. Nach seiner Ansicht ist für einen effizienten Schutz der Grundrechte Betroffener gegenüber Eingriffen in ihre Privatsphäre eine weite Auslegung der Bestimmung zur Anwendbarkeit nationalen Rechts erforderlich. Das hatte der EuGH bereits in zwei vorangegangenen Entscheidungen klargestellt: „Ich gehe davon aus, dass das europäische Gericht die Auffassung aller europäischen Datenschutzbehörden bestätigt und seine bisherige Rechtsprechung weiter verfolgen wird. Das Verfahren zum Klarnamenzwang geht juristisch in die nächste Runde“ (HmbBfDI, Pseudonyme Nutzung bei Facebook weiter ungeklärt, PE 01.07.2016; Facebook

darf Pseudonyme verbieten - Schlappe für Datenschützer, www.onvista.de 01.07.2016; http://justiz.hamburg.de/contentblob/6472090/721e732f31b252c738c46e4acef22b09/data/5bs40-16.pdf).

OVG Schleswig-Holstein

Digitalisierung von Personalakten im Auftrag unzulässig

Das Schleswig-Holsteinische Oberverwaltungsgericht (OVG) hat mit Beschluss vom 27.07.2016 entschieden, dass die Digitalisierung von Personalakten der Landesbeamtinnen und Landesbeamten durch einen privaten Unterauftragnehmer unzulässig ist (Az. 2 MB 11/16). Ein Landesbeamter hatte der beabsichtigten Digitalisierung seiner Personalakte durch einen externen Scan-Dienstleister widersprochen und zunächst erfolglos beim Verwaltungsgericht um einstweiligen Rechtsschutz nachgesucht. Auf seine Beschwerde hin untersagte das OVG die Herausgabe seiner Personalakten. Es fehle an einer gesetzlichen Grundlage im Beamtenrecht, die die Weitergabe von Personalakten an externe Stellen erlaubt. Bei den beamtenrechtlichen Vorschriften zur Vertraulichkeit und Zweckbindung der Personalakte (§ 50 Beamtenstatusgesetz u. §§ 85 ff. Landesbeamtengesetz) handele es sich um abschließende Regelungen zum Umgang mit personenbezogenen Daten in Personalakten. Danach ist der Zugang zu Personalakten nur einem begrenzten Personenkreis möglich. Um diesen Personenkreis zu erweitern – etwa zum Zwecke des Einscannens der Personalakten durch ein privates Unternehmen – hätte es einer gesetzlichen Grundlage bedurft. Die Vorschriften des § 17 Landesdatenschutzgesetz zur Verarbeitung personenbezogener Daten im Auftrag seien für die Behandlung von Personalakten wegen des abschließenden Charakters des Landesbeamtengesetzes nicht anwendbar. Ob dies auch für andere Beschäftigte im öffentlichen Dienst wegen der auf die beamtenrechtlichen Vorschriften verweisenden Regelung des § 23 Abs. 1 Landesdatenschutzgesetz gilt, wurde vom Gericht nicht entschieden.

Bislang waren bereits Unterlagen von 36.000 Mitarbeitenden elektronisch erfasst, u. a. die Akten der 29.000 Lehrkräfte des Landes. In der Staatskanzlei, so der Leiter für Informationstechnik Sven Thomsen, hatte man sich auf der sicheren Seite gewähnt, da das Vorgehen nicht nur mit allen Ministerien, sondern auch mit dem Grundsatzreferat für Beamtenrecht, den Spitzenorganisationen der Gewerkschaften und dem Unabhängigen Landeszentrum für Datenschutz abgestimmt worden war. Die Staatskanzlei will jetzt das Landesbeamtengesetz so schnell wie möglich ändern lassen, um wie bisher weitermachen zu können. Die Personalakte eines Beschäftigten umfasst im Schnitt 350 Seiten. Die Landesregierung hatte im Mai 2015 beschlossen, die Unterlagen künftig ausschließlich elektronisch zu führen. Der Landes-IT-Dienstleister Dataport vergab den Unterauftrag an Rhenus Office Systems, das sich auf solche Aufgaben spezialisiert hat. Dessen Beschäftigte scannten bis zu 1.000 Personalakten pro Woche ein und signieren dabei die erfassten Seiten so, dass sie nachträglich nicht unerkannt verändert werden können. Thomsen geht von einer viermonatigen Verzögerung und einem finanziellen Schaden von bis zu 300.000 € aus: „Das ist ärgerlich, weil wir das Projekt engagiert und stringent geplant haben.“ Schleswig-Holstein sei mit seiner Digitalisierung Pionier, weshalb andere Bundesländer interessiert nach Kiel blicken würden (Hiersemenzel, Personalakten zurück in Beamtenhand, Kieler Nachrichten, 30.07.2016, 10; Oberverwaltungsgericht Schleswig untersagt im Eilrechtsschutzverfahren die Digitalisierung der Personalakte eines Landesbeamten durch einen Unterauftragnehmer, http://www.schleswig-holstein.de, 28.07.2016).

KG Berlin

WhatsApp muss AGB in Deutsch anbieten

Das Berliner Kammergericht (KG) hat dem Messenger-Dienst WhatsApp mit Urteil vom 08.04.2016 untersagt, auf seiner deutschen Internetseite nur englischsprachige Allgemeine Geschäftsbedingungen (AGB) zu verwenden (5-U-156/14). Damit gaben die Richter einer Klage des Verbraucherzentrale Bundesverbands (vzbv) gegen das in Kalifornien ansässige Unternehmen statt. Der vzbv hatte kritisiert, dass die seitenlangen und mit Fachausdrücken gespickten Nutzungsbedingen für VerbraucherInnen aus Deutschland weitgehend unverständlich sind.

WhatsApp, das seit 2014 zu Facebook gehört, wirbt auf seiner ansonsten deutschsprachigen Internetseite um KundInnen für seinen Messenger-Dienst. Nachrichten schreiben per Whatsapp ist laut Selbstdarstellung nicht nur „einfach“, sondern auch „persönlich“. Dies gilt aber nicht für Nachrichten an das Unternehmen. Wer Whatsapp nutzen möchte, muss sich zunächst registrieren und den nur in englischer Sprache verfügbaren Nutzungsbedingungen und der englischsprachigen Datenschutzrichtlinie (20 DIN-A4-Seiten) zustimmen. Der Text enthält eine Vielzahl von Freigabeerklärungen. So erlaubt der Text dem Unternehmen, die Telefonkontakte der KundInnen zu durchsuchen und seine Status-Texte für geschäftliche Zwecke zu verwenden. Aus den Daten, die Whatsapp mit verschiedenen Analysemethoden sammelt, darf der Dienst gemäß dem Kleingedruckten die Vorlieben der KundInnen ermitteln und seinen Service entsprechend anpassen. Nutzende müssen bestätigen, dass sie älter als 16 Jahre seien. Wenn sich Whatsapp mit einem anderen Unternehmen zusammenschließt oder seinen Dienst an eine andere Firma verkauft, gehen alle gespeicherten Nutzungsdaten an das andere Unternehmen über. All das wird ausschließlich in Englisch beschrieben.

Das KG schloss sich der Auffassung des vzbv an, dass diese Praxis für VerbraucherInnen nicht zumutbar, intransparent und benachteiligend für deutschen Nutzerinnen ist. Alltagsenglisch sei hierzulande zwar verbreitet, nicht aber juristisches, vertragssprachliches und kommerzielles Englisch. Kein Kunde müsse damit rechnen, „einem umfangreichen, komplexen Regelwerk mit sehr, sehr vielen Klauseln“ in einer Fremdsprache ausgesetzt zu sein. Solange die Bedingungen nicht ins Deutsche übersetzt sind, seien sämtliche Klauseln intransparent und damit unwirksam. Wird das Urteil rechtskräftig, muss WhatsApp die Nutzungsbedingungen und Datenschutzhinweise in deutscher Fassung bereitstellen.

Tut das Unternehmen dies nicht, so droht ein Ordnungsgeld von bis zu 250.000 €.

Die Richter monierten außerdem einen Verstoß gegen das Telemediengesetz (TMG). Nach § 5 Abs. 1 Nr. 2 TMG müssen Anbieter neben einer E-Mail-Adresse eine zweite Möglichkeit zu einer schnellen und unmittelbaren Kontaktaufnahme angeben, zum Beispiel ein Kontaktformular oder eine Telefonnummer, unter der die Firma zu erreichen ist. Diese zweite Möglichkeit fehlte bei WhatsApp. Das Unternehmen hatte zwar einen Link auf seine Seiten bei Facebook und Twitter gesetzt. Doch über Twitter können Nutzer keine Nachrichten an das Unternehmen senden. Und sein Facebook-Profil hatte WhatsApp so eingerichtet, dass die Zusendung einer Nachricht ausgeschlossen war.

Whatsapp hat kein Büro in Deutschland. Trotzdem sind deutsche Gerichte zuständig, da sich deren Werbung explizit an deutsche KundInnen richtet. Nicht durchdringen konnte der vzbv dagegen mit seiner Auffassung, dass im Impressum auch ein Vertretungsberechtigter des Unternehmens genannt werden muss. Das Gericht urteilte, dass dem europäischen Recht entsprechend nur die Nennung des Namens und der Anschrift des Diensteanbieters vorgeschrieben sei. Das Kammergericht hat keine Revision gegen das Urteil zugelassen. WhatsApp kann dagegen aber noch eine Nichtzulassungsbeschwerde beim Bundesgerichtshof einlegen.

Klaus Müller, Vorstand des vzbv, begrüßte das Urteil: „AGB von Unternehmen sind ohnehin oft lang und für Verbraucher schwer verständlich. Dass die Millionen deutschen Nutzer von WhatsApp diese nicht auch noch in einer fremden Sprache hinnehmen müssen, ist auch ein wichtiges Signal an andere international handelnde Unternehmen.“ (vzbv, PE 17.05.2016, WhatsApp muss AGB auf Deutsch bereitstellen; Ludwig, Was ist los? SZ 17.05.2016).

OLG Stuttgart

Kein Dashcam-Verwertungsverbot bei OWi-Verfahren

Der Senat für Bußgeldsachen des Oberlandesgerichts (OLG) Stuttgart hat es mit rechtskräftigem Beschluss vom 04.05.2015 für grundsätzlich zulässig erachtet, in einem Bußgeldverfahren ein Video zu verwerten, das ein anderer Verkehrsteilnehmer mit einer „Dashcam“ aufgenommen hat (4 Ss 543/15, Vorinstanz Amtsgericht – AG – Reutlingen, U. v. 27.05.2015 – 7 OWi 28 Js 7406/15). Dies gelte jedenfalls für die Verfolgung schwerwiegender Verkehrsordnungswidrigkeiten wie – vorliegend – eines Rotlichtverstoßes an einer mindestens seit sechs Sekunden rot zeigenden Ampel. Als „Dashcam“ wird eine auf dem Armaturenbrett oder an der Windschutzscheibe eines Fahrzeugs angebrachte Videokamera bezeichnet, die während der Fahrt aufnimmt.

Das AG Reutlingen hatte gegen den Betroffenen wegen einer fahrlässigen Ordnungswidrigkeit des Missachtens des Rotlichts einer Ampel eine Geldbuße von 200 Euro und ein Fahrverbot von einem Monat verhängt. Den Tatnachweis konnte das Amtsgericht allein aufgrund eines Videos führen, das ein anderer Verkehrsteilnehmer zunächst anlasslos mit einer „Dashcam“ aufgenommen hatte. Das OLG verwarf die Rechtsbeschwerde des Betroffenen und bestätigte das Urteil.

Der Senat ließ es offen, ob bzw. unter welchen Umständen die Nutzung einer „Dashcam“ durch einen Verkehrsteilnehmer gegen § 6b des Bundesdatenschutzgesetzes (BDSG) verstößt, der die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur in engen Grenzen zulässt. Jedenfalls enthalte § 6b Abs. 3 Satz 2 BDSG kein Beweisverwertungsverbot für das Straf- und Bußgeldverfahren. Somit folge aus einem (möglichen) Verstoß gegen diese Vorschrift nicht zwingend eine Unverwertbarkeit der Videoaufnahme. Über die Verwertbarkeit sei vielmehr im Einzelfall unter Abwägung der widerstreitenden Interessen zu entscheiden.

Dass das AG im vorliegenden Fall kein Beweisverwertungsverbot angenommen habe, sei aus Rechtsgründen nicht zu beanstanden. Zwar griffen Videoaufnahmen von Verkehrsvorgängen in das allgemeine Persönlichkeitsrecht des Betroffenen aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein. Die Intensität und Reichweite des Eingriffs sei im konkreten Fall jedoch gering. Insbesondere betreffe ein Video, das lediglich Verkehrsvorgänge dokumentiere und mittelbar die Identifizierung des Betroffenen über das Kennzeichen seines Fahrzeugs ermögliche, nicht den Kernbereich seiner privaten Lebensgestaltung oder seine engere Privat- oder gar Intimsphäre. Im Rahmen der Abwägung seien zudem die hohe Bedeutung der Verfolgung schwerer Verkehrsverstöße für die Sicherheit des Straßenverkehrs und das Gewicht des Verstoßes im Einzelfall zu berücksichtigen.

Das OLG hob hervor, dass die Bußgeldbehörden ihrerseits bereits bei Verfahrenseinleitung die Verwertbarkeit derartiger Aufnahmen zu prüfen und u. a. die Schwere des Eingriffs gegen die Bedeutung und das Gewicht der angezeigten Ordnungswidrigkeit abzuwägen hätten. So betonte auch Hannes Krämer, Justiziar des Automobilclubs ACE, dass es auf den Einzelfall ankäme, weshalb auch die Polizei keine Flut von Anzeigen durch Denunzianten auf sich zukommen sieht, so Oliver Malchow, Chef der Polizeigewerkschaft GdP: „Wir wollen keine Bespitzelung“. Dieser Aussage schloss sich auch der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) an. Aufgrund des Opportunitätsgrundsatzes (vgl. § 47 OWiG) stehe es den Bußgeldbehörden frei, ein ausschließlich auf der Ermittlungstätigkeit von Privaten mittels „Dashcam“ beruhendes Verfahren nicht weiter zu verfolgen. Rechtsfragen, die sich beim Einsatz von „Dashcams“ stellen, sind in der Rechtsprechung und der Literatur stark umstritten und werden uneinheitlich beantwortet. Auch der 54. Deutsche Verkehrsgerichtstag hatte sich im Januar 2016 mit dieser Thematik befasst (PE OLG Stuttgart, 18.05.2016, „Dashcam“-Aufnahmen können zur Verfolgung schwerwiegender Verkehrsordnungswidrigkeiten grundsätzlich verwertet werden; Temsch, Spione an der Scheibe, SZ 20.05.2016, 1).

LG Frankfurt

Informationspflicht für TV-Gerätehersteller über Datenerhebung

Das Landgericht (LG) Frankfurt a. M. verurteilte auf die Klage der Verbraucherzentrale Nordrhein-Westfalen (VZ NRW) den Smart-TV-

Hersteller Samsung, die KäuferInnen seiner Smart-TV darauf hinzuweisen, dass beim Anschluss des Fernsehers ans Internet personenbezogene Daten erhoben und verwendet werden können (Urt. v. 10.06.2016, Az. 2-03 O 364/15). Zugleich untersagte das Gericht am Freitag die Verwendung zahlreicher Klauseln in den Allgemeinen Geschäftsbedingungen (AGB) wegen mangelnder Transparenz. Die VZ NRW warf Samsung vor, Kundendaten ohne Einwilligung der Betroffenen an die Firmenserver zu senden, sobald ein Gerät mit dem Internet verbunden wird. Mit ihrer Musterklage zielte die VZ NRW darauf ab, Daten erst nach entsprechender Information durch die Gerätehersteller und nach Einwilligung der NutzerInnen zu übertragen.

Soweit Samsung die Erhebung personenbezogener Daten im Rahmen der Nutzung des sogenannten HbbTV-Dienstes bei Smart-TVs sowie der Einrichtung des Smart-TVs ohne vorherige Zustimmung untersagt werden sollte, hat das Gericht die Klage jedoch abgewiesen. Diese Daten würden nicht an die verklagte deutsche Gesellschaft, sondern vielmehr an die Betreiber der HbbTV-Dienste einerseits und die nicht verklagte ausländische Konzernmutter andererseits übermittelt werden. Ob die Datenübermittlung in der konkreten Art und Weise rechtmäßig war, wurde daher von der Kammer nicht entschieden.

Samsung wurde jedoch verurteilt, KäuferInnen eines Smart-TV darauf hinzuweisen, dass bei Anschluss des Smart-TV an das Internet die Gefahr besteht, dass personenbezogene Daten des Verbrauchers erhoben und verwendet werden. Hierbei ist das Gericht davon ausgegangen, dass es einem Teil der Verbraucher, die ein solches Smart-TV-Gerät erwerben, nicht bekannt ist, dass nach Anschluss des Geräts personenbezogene Daten in Form von IP-Adressen auch dann erhoben werden können, wenn die Internet-Funktionalität des Smart-TV überhaupt nicht genutzt wird. Dem Verbraucher sei in der Regel nicht bekannt, dass über die HbbTV-Funktion des Smart-TV Fernsehsender personenbezogene Daten in Form von IP-Adressen erheben können.

Die Klage hatte weiterhin Erfolg, soweit sie die AGBs von Samsung und die konkrete Form der Datenschutzerklärungen betraf. Das Gericht hat es als unzumutbar angesehen, dass diese auf jeweils über 50 Bildschirmseiten präsentiert werden und zu lang und nicht hinreichend lesefreundlich aufbereitet sind. Darüber hinaus wurde Samsung die Verwendung einer Vielzahl von Klauseln in ihren AGBs untersagt. Gründe hierfür waren die nicht ausreichende Bestimmtheit und Transparenz im Hinblick auf den Umfang der Datenübermittlung und -verwendung (Teilsieg für NRW-Verbraucherschützer, www.lto.de 10.06.2016).

Buchbesprechungen



Wedde, Peter (Hrsg.)
Handbuch Datenschutz und Mitbestimmung
Bund Verlag Frankfurt/Mai 2016, 417 S., 49,90 €
ISBN 978-3-7663-6442-5,

(tw) Der Bund-Verlag ist bekannt für seine arbeitnehmerorientierte Fachliteratur, die sich an Betriebs- und Personalräte richtet. Mit dem neuen von Peter Wedde herausgegebenen Werk ergänzt der Verlag sein Portfolio beim Datenschutz. Es gibt einen umfassenden Ein- und Überblick zum Beschäftigtendatenschutz und beschränkt sich nicht, wie der Titel suggeriert, auf die kollektivrechtliche Seite. Zwar titelt es als „Handbuch", tatsächlich geeignet ist es auch als Einführung und Lehrbuch. Die AutorInnen Stefan Brink, Isabel Eder, Nadja Häfner-Beil, Heinz-Peter Höller, Silvia Mittländer, Marc-Oliver Schulze, Regian Steiner und der Herausgeber erklären den Datenschutz von der Pike auf, indem sie erst dessen Grundlagen, deren individual- und dann deren kollektivrechtliche Seite und die spezifische Rolle des Datenschutzbeauftragten beleuchten. In den letzten beiden Kapiteln befasst sich das Werk mit Einzelthemen (Leistungs- und Verhaltenskontrollen, Bewerbung, Arbeitsvertrag, Personalakte, Gesundheitsdaten, Betriebsübergang und Rechtsverstöße) und neuen Technologien (Personal-DV, Kommunikationsdienste, Internet, Mobilität, Business Intelligence, Industrie 4.0 und E-Learning). Diese vertiefenden Teile finden sich so in anderen vergleichbaren Werken nicht. Der Anhang führt die Adressen der Datenschutzbehörden und ein ausführliches Stichwortverzeichnis.

Die Neuerungen durch die Datenschutz-Grundverordnung werden zwar erwähnt, aber nicht ausführlich dargestellt. Die Besonderheit liegt weniger im Juristischen, dass hinreichend dargestellt wird, sondern in der Praxisver-

mittlung, wozu viele anschauliche Beispielfälle und Checklisten nützlich sind, und in der verständlichen Darstellung. Die Quellenverweise sind eher sparsam. Dies hindert PraktikerInnen aber nicht, das Werk als Handbuch und Nachschlagewerk zu nutzen.



Laue, Philip / Nink, Judith / Kremer, Sascha
Das Neue Datenschutzrecht in der betrieblichen Praxis
Nomos Verlagsgesellschaft Baden-Baden 2016, 326 S., 48,00 €
ISBN 978-3-8487-2377-5

(tw) Das Rennen hat begonnen: Kaum ist der endgültige Text der Europäischen Datenschutz-Grundverordnung (DSGVO) fixiert, hat der Kampf um deren Interpretation und um die frühestmögliche Kommentierung begonnen. Tatsächlich dürfte es kaum eine europäische Regelung geben, zu der in kürzester Zeit vergleichbar viele Interpretationsangebote auf dem Meinungsmarkt der Fachpresse geworfen wurden und werden. Es geht auch um viel – um die Auslegung der ersten europäischen direkt verbindlichen Regeln zur personenbezogenen Datenverarbeitung; letztlich geht es um die Rahmenbedingungen eines riesigen und weiter zunehmenden Geschäftszweigs der digitalen Informationsgesellschaft. Wer als Erster qualifiziert auf dem Markt ist, wird zitiert und gibt Meinungen, Schwerpunkte und Niveau der Auseinandersetzung vor.

Insofern ist dem Buch von Laue/Nink/Kremer ein erster Platz wohl nicht streitig zu machen: Es handelt sich, nach der Veröffentlichung von vielen Fachaufsätzen, um die erste umfassende und umfangreiche systematische Darstellung der DSGVO. Angesichts eines Redaktionsschlusses von Juli 2016 (berücksichtigt sind nicht nur das Inkrafttreten der DSGVO, sondern z. B. auch – zumindest als in Form einer kurzen inhaltlichen Erwähnung – das Privacy Shield) ist die Herausgabe Anfang August 2018 wohl ein Meisterwerk nicht nur von den AutorInnen, sondern auch von Verlag, Herstellung und Vertrieb. Überraschend ist dann nicht nur die Geschwindigkeit, sondern auch Umfang und Qualität des Inhalts. Das Buch enthält eine gediegene Erstkommentierung der DSGVO, bei der nicht nur einige BDSG-Kommentierungen, sondern auch die aktuelle Literatur sehr weitgehend berücksichtigt wird. Dabei greift es die dort geführten Diskussionen auf und vertritt eigene Meinungen unter ausführlichem Rückgriff auf den Text und die Erwägungsgründe der DSGVO. Dies wird in den aktuellen rechtlichen Kontext, vom bestehenden BDSG über das TMG bis hin zur Rechtsprechung und zum Schrifttum, gestellt. Die Streitstände werden nachvollziehbar dargestellt und bewertet, wobei eine eher praxis- und verarbeitungsfreundliche pragmatische Linie verfolgt wird, die am Bekannten (nämlich der bisherigen BDSG-Interpretation) anknüpft.

Dennoch kann der Buchtitel missverstanden werden. „Betriebliche Praxis“ sollte weniger im Sinne von Geschäftsleitungen, Betriebsräten oder allgemeines Unternehmens-Justiziariat verstanden werden, sondern eher als „Datenschutzjuristen“. Die Ausführungen sind vorrangig rechts- und nicht technikbezogen, teilweise sehr abstrakt und voraussetzungsvoll. Zwar enthält das Buch eingängige Beispiele und Hinweise für die Praxis. Adressiert werden aber eher juristisch vorgebildete externe, interne, unabhängige, interessierte … DatenschützerInnen. Denen werden nun keine Patentrezepte geliefert, sondern erste DSGVO-Erläuterungen, wobei auf Vorläufigkeiten und Unklarheiten hingewiesen wird. Das deutsche Umsetzungsgesetz – selbst als Entwurf – lag ja auch noch nicht vor. Abgedeckt wird also bei weitem nicht das Datenschutzrecht insgesamt, sondern werden die Neuigkeiten durch die DSGVO. Nicht nur im Stichwortverzeichnis, sondern auch im Text finden sich einige relevante Anwendungen nicht oder nur ganz am Rande, z. B. Videoüberwachung, Auskunfteien, Gesundheits- oder Sozialdatenverarbeitung.

Das Buch ist insofern äußerst wert- und verdienstvoll, dass es die komplizierte Suche der verstreuten aktuellen Fachartikeln weitgehend unnötig macht und hierauf präzise verweist. Die Verzeichnisse (Inhalt, Literatur, Stichworte) sind praktikabel und hilfreich. Für einen ersten Einstieg in und einen Überblick über die DSGVO ist das Buch schon zu detailliert. Als Handbuch und Nachschlagewerk und Recherchehilfe ist es, nicht nur für die betriebliche Praxis, hervorragend geeignet.



Härting, Niko
Datenschutz-Grundverordnung - Das Neue Datenschutzrecht in der betrieblichen Praxis
ottoschmidt Verlag Köln 2016, 198 S., 39,80 €
ISBN 978-3-504-42059-8

(tw) Zu den schnellen Kommentierern der Datenschutz-Grundverordnung (DSGVO) gehört auch Niko Härting, der während der Entstehungsphase der DSGVO immer wieder zum Ausdruck gebracht hat, dass ihm die Richtung, die EU-Kommission und -Parlament zum Thema eingeschlagen haben, überhaupt nicht passt. Dies verheimlicht er auch nicht in seinem Vorwort. Umso erfreulicher ist die dogmatisch qualifizierte Ausarbeitung. In „über 100 Fragen und Antworten“ behandelt auch er – so wie der Titel von Laue/Nink/Kremer (s. o.) – „das neue Datenschutzrecht in der betrieblichen Praxis“, wobei hier der Untertitel das hält, was er ankündigt: Bezogen auf die praktische Anwendung der

DSGVO behandelt Härting systematisch – manchmal etwas zu stichwort- und aufzählungsartig – alle wichtigen Datenschutzfragen im Unternehmen. Dabei orientiert er sich weder an der Systematik der DSGVO noch der des BDSG, sondern strukturiert nach betrieblichen Fragestellungen: Compliance (bDSB, Folgenabschätzung, Transparenz, Risikoorientierung, technisch-organisatorische Maßnahmen, Datenpannen, Auslandstransfer, Anwendungsbereich, Haftung und Sanktionen), materielles Datenschutzrecht, Cloud Computing und Big Data sowie Betroffenenrechte, Aufsicht und Selbstregulierung.

Bei seiner Darstellung gibt er zu den einzelnen Themen jeweils eine Fragestellung vor, die er erst gemäß dem derzeit noch anwendbaren Recht, also insbesondere dem BDSG, beantwortet, um dann die Änderungen durch die DSGVO darzustellen, wobei er ausführlich auch Normtext und Erwägungsgründe zitiert, Querverweise herstellt und danach interpretiert. Dies macht er in einer Sprache, die in Unternehmen auch von Nicht-JuristInnen verstanden werden kann. Wesentliches hält er zusätzlich in Merksätzen fest. Dabei bleibt Härting seinem Ruf treu, regelmäßig sehr verarbeitungsfreundliche Interpretationen zu geben, etwa wenn er meint, dass in Art. 6 Abs. 4 die bisherigen eher strengen Zweckbindungsregeln aufgeweicht würden oder wenn er in der Verwendung des Begriffs „vernünftige Erwartungen" bei der Interessenabwägung eine inhaltliche Nähe zum „reasonable expectations of privacy test" des US-Rechts suggeriert. Verblüffend ist, dass er im Hinblick auf Big Data oder Scoring in Art. 22 eine eher enge Auslegung präferiert.

Härtings Darstellung bezieht sich bewusst ausschließlich auf die DSGVO, dies aber umfassend, etwa durch Herstellung von Bezügen auch zum Telemediengesetz. Dabei hat er die im Betrieb für die Anpassung an das neue Recht Zuständigen im Blick, ohne aber in Checklisten oder Patentrezepten zu verkürzen. Er verzichtet bewusst – abgesehen von einigen zentralen Gerichtsentscheidungen – auf weiteren Quellenhinweise. Ein relativ kurzes Stichwortverzeichnis ermöglicht beim gezielten Suchen das Auffinden relevanter Stellen. Das Buch ist also geeignet, Licht in die neue und für die meisten noch ungewohnte Materie der DSGVO für Praxisanwendungen zu bringen. Eine grundrechtsorientierte LeserIn des Buchs sollte die Verfassungsaspekte mitdenken, die bei der zweifellos normdogmatisch stringenten Argumentation der Darstellung eher zu kurz kommen.



Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin/Nink, David/Weinzierl, Quirin/Wenzel, Michael
Die Datenschutz-Grundverordnung und das nationale Recht – Erste Überlegungen zum innerstaatlichen Regelungsbedarf
Monsenstein Vannerdat Münster, 2016, 525 S., im Internet abrufbar unter http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf

(tw) Nicht für die Datenschutzpraxis, wohl aber für Gesetzgeber, Lobbyvertreter und Wissenschaft nützlich ist das auch im Internet veröffentlichte Rechtsgutachten, das sich mit den von der Datenschutz-Grundverordnung (DSGVO) ermöglichten und geforderten nationalen Regelungen befasst. Das Gutachten wurde für das auf Bundesebene mit dem Datenschutzrecht federführend betraute Bundesministerium des Innern (BMI) erstellt, um die sich aus der DSGVO ergebenden Handlungsspielräume und -pflichten auszuloten. Bevor sich das Gutachten mit den 49 Passagen der DSGVO (Erwägungsgründe und Artikel-Regelungen) befasst, die Mitgliedstaaten zu Regelungen ermuntern, werden die Hintergründe für den Erlass der DSGVO als Richtlinie, die unionsrechtlichen Steuerungsvorgaben für (echte und unechte) Öffnungsklauseln sowie deren Typologie dargelegt und in einer Übersichtstabelle der DSGVO zugeordnet.

In einem weiteren Schritt nimmt sich das Gutachten aller Regelungen des derzeit bestehenden BDSG an und untersucht, inwieweit diese beibehalten werden können oder müssen, was auch übersichtlich in entsprechenden Tabellen abgebildet wird. Das Gutachten ist eine wichtige Fleißarbeit, mit der der Rahmen der nötigen nationalen Datenschutzregelungen dargestellt wird. Ist die DSGVO unklar, so verweist das Gutachten hierauf und gibt regelmäßig praktikable Empfehlungen (vgl. dazu auch Digitalcourage/DVD DANA 2016, 86 f. sowie die weiteren Stellungnahmen im Heft DANA 2/2016). Nicht Thema des Gutachtens sind Regelungsbedarfe, die sich nicht aus der DSGVO bzw. dem bisherigen BDSG ergeben. Diese geraten leider bei der aktuellen Diskussion verstärkt aus dem Blickfeld (dazu Netzwerk Datenschutzexpertise, Datenschutzrechtlicher Handlungsbedarf 2016 für die deutsche Politik nach Verabschiedung der EU-DSGVO http://www.netzwerk-datenschutzexpertise.de/sites/default/files/empf_2016_nat_regelungsbedarf.pdf).

online zu bestellen unter: **www.datenschutzverein.de/dana**

G_H_IMDI_NST_ VOR G_RICHT

KRIMINELLE V-LEUTE, ILLEGALE ABHÖRPRAKTIKEN,
MACHTLOSE KONTROLLEURE.
WAS MUSS SICH ÄNDERN?

22.10.16

Forum Geheimdienste und Demokratie
10 Uhr | Humboldt-Universität
Theaterinszenierung
19.30 Uhr | Maxim Gorki Theater

www.geheimdienste-vor-gericht.de



In Kooperation mit:







Gefördert von:





